PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-288453
(43)Date of publication of application : 04.10.2002

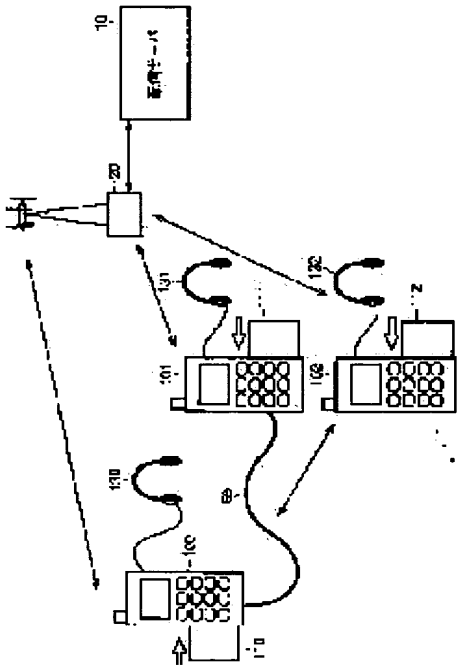
(51)Int.Cl. G06F 17/60
G06F 12/00
G06F 12/14
G06F 17/30
H04Q 7/38
H04L 9/08

(21)Application number : 2001-090489
(22)Date of filing : 27.03.2001

(71)Applicant : SANYO ELECTRIC CO LTD
(72)Inventor : YASUDA CHOMEI

(54) INFORMATION TERMINAL

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an information terminal which retrieves a storage place on of ciphered contents data, which a user wants to acquire, and acquires ciphered contents data from this retrieved storage place.
SOLUTION: When wanting to newly purchase music of an artist A, the user of a mobile phone 100 receives the retrieval result of the artist A from a delivery server 10. The mobile phone 100 retrieves a memory card, where ciphered contents data included in the retrieval result received from the delivery server 10 is stored, on the basis of a database. When ciphered contents data is stored in a memory card 111, the mobile phone 100 copies ciphered contents data from a mobile phone 101 and receives a license from the delivery server 10.



LEGAL STATUS

[Date of request for examination] 05.08.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

BEST AVAILABLE COPY

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－288453
（P2002－288453A）
(43)公開日　平成14年10月４日(2002.10.4)

(51)Int.Cl.'		識別記号	F I		テーマコード'(参考)
Ｇ０６Ｆ	17/60	３０２	Ｇ０６Ｆ 17/60	３０２Ｅ	５Ｂ０１７
		ＺＥＣ		ＺＥＣ	５Ｂ０７５
		１４２		１４２	５Ｂ０８２
		５０２		５０２	５Ｊ１０４
	12/00	５４５	12/00	５４５Ｚ	５Ｋ０６７

審査請求　未請求　請求項の数６　ＯＬ　（全 26 頁）　最終頁に続く

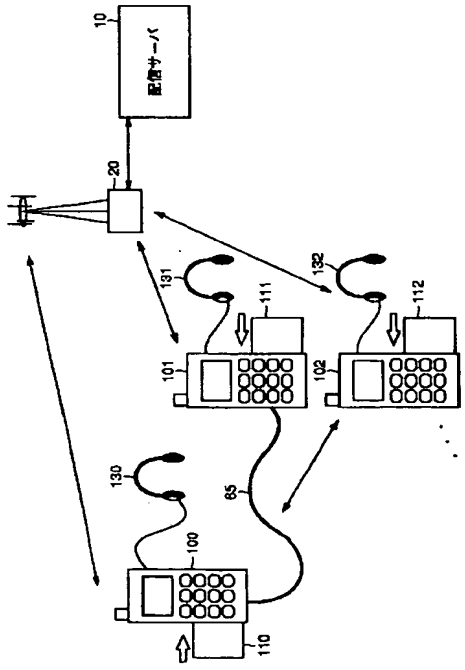
(21)出願番号　特願2001－90489(P2001－90489)
(22)出願日　平成13年３月27日(2001.3.27)

(71)出願人　000001889
三洋電機株式会社
大阪府守口市京阪本通２丁目５番５号
(72)発明者　安田　朝明
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(74)代理人　100064746
弁理士　深見　久郎　（外３名）

最終頁に続く

(54)【発明の名称】　情報端末装置

(57)【要約】
【課題】　ユーザが取得したい暗号化コンテンツデータの格納場所を検索し、その検索した格納場所から暗号化コンテンツデータを取得する情報端末装置を提供する。
【解決手段】　携帯電話機１００のユーザは、新たにアーティストＡの曲を購入したいとき、そのアーティストＡの検索結果を配信サーバ１０から受信する。携帯電話機１００は配信サーバ１０から受信した検索結果に含まれる暗号化コンテンツデータがどのメモリカードに格納されているかをデータベースに基づいて検索する。そして、携帯電話機１００は、暗号化コンテンツデータがメモリカード１１１に格納されているとき携帯電話機１０１から暗号化コンテンツデータをコピーし、ライセンスを配信サーバ１０から受信する。



1

【特許請求の範囲】

【請求項１】　複数の情報端末装置において作成され、かつ、暗号化コンテンツデータを管理するための複数のベータベースを検索して前記暗号化コンテンツデータと前記暗号化コンテンツデータを再生するためのライセンスとを取得する情報端末装置であって、

外部とのデータのやり取りを行なう送受信部と、

指示を入力するためのキー操作部と、

前記複数のデータベースと一覧表とを記憶する記憶部と、

制御部とを備え、

前記複数のデータベースの各々は、複数の暗号化コンテンツデータを特定するための複数のコンテンツ特定情報と、前記暗号化コンテンツデータに対応するライセンスの有無を示す複数のライセンス情報と、前記暗号化コンテンツデータおよび前記ライセンスが記録されたデータ記録装置を特定するための複数の記録装置特定情報とを含み、

前記一覧表は、前記複数のベータベースを特定するための複数のデータベース特定情報と、前記複数のデータベースの各々が生成された情報端末装置を特定するための複数の端末特定情報とを含み、

前記制御部は、前記暗号化コンテンツデータの購入要求に応じて、前記キー操作部を介して入力された購入コンテンツの検索条件を前記送受信部を介して配信サーバへ送信し、前記検索条件に合致するコンテンツのコンテンツ特定情報を前記配信サーバから前記送受信部を介して受信し、その受信したコンテンツ特定情報に一致するコンテンツ特定情報と前記一致したコンテンツ特定情報に対応するライセンス情報および端末特定情報とを前記複数のデータベースおよび前記一覧表から抽出し、その抽出したコンテンツ特定情報、ライセンス情報および端末特定情報を含む検索結果データベースを作成する、情報端末装置。

【請求項２】　各種の情報を視覚情報としてユーザに与えるための表示部をさらに備え、

前記制御部は、コンテンツ特定情報、ライセンス情報、および端末特定情報を前記検索結果データベースから読出して前記表示部に表示し、前記キー操作部を介して他の情報端末装置が保持する暗号化コンテンツデータの選択が入力されると、前記他の情報端末装置へ前記暗号化コンテンツデータの複製依頼を前記送受信部を介して送信し、前記他の情報端末装置において前記複製が許可されると前記他の情報端末装置から前記暗号化コンテンツデータを前記送受信部を介して受信する、請求項１に記載の情報端末装置。

【請求項３】　前記制御部は、さらに、前記取得要求された暗号化コンテンツデータに対応するライセンス情報がライセンスの無しを表すとき、前記配信サーバから前記複製された暗号化コンテンツデータに対応するライセンスを受信する、請求項２に記載の情報端末装置。

2

【請求項４】　各種の情報を視覚情報としてユーザに与えるための表示部と、

前記データ記録装置との間のやり取りを制御するインタフェースとをさらに備え、

前記制御部は、コンテンツ特定情報、ライセンス情報、および端末特定情報を前記検索結果データベースから読出して前記表示部に表示し、自己がやり取りを行なうデータ記録装置に記録された暗号化コンテンツデータの選択が前記キー操作部を介して入力され、前記選択された暗号化コンテンツデータに対応するライセンス情報がライセンスの無しを表すとき前記ライセンスの送信依頼を前記送受信部を介して前記配信サーバへ送信し、前記配信サーバから前記ライセンスを前記送受信部を介して受信する、請求項１に記載の情報端末装置。

【請求項５】　各種の情報を視覚情報としてユーザに与えるための表示部と、

前記データ記録装置との間のやり取りを制御するインタフェースとをさらに備え、

前記制御部は、コンテンツ特定情報、ライセンス情報、および端末特定情報を前記検索結果データベースから読出して前記表示部に表示し、前記配信サーバが保持する暗号化コンテンツデータの選択が前記キー操作部を介して入力されたとき前記選択された暗号化コンテンツデータおよび前記選択された暗号化コンテンツデータに対応するライセンスの送信依頼を前記送受信部を介して前記配信サーバへ送信し、前記配信サーバから前記暗号化コンテンツデータおよびライセンスを前記送受信部を介して受信する、請求項１に記載の情報端末装置。

【請求項６】　前記制御部は、さらに、データベースの取得要求に応じて他の情報端末装置が保持するデータベースを前記他の情報端末装置から前記送受信部を介して受信し、その受信したデータベースを前記記憶部に格納するとともに前記格納したデータベースを追加して前記一覧表を更新する、請求項１から請求項５のいずれか１項に記載の情報端末装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、コンテンツデータを管理するための複数のデータベースを保持し、コンテンツデータの取得要求に応じて複数のデータベースを検索してコンテンツデータを取得する情報端末装置に関するものである。

【０００２】

【従来の技術】近年、インターネット等のデジタル情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【０００３】このようなデジタル情報通信網においては、デジタル信号により情報が伝送される。したがっ

て、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【０００４】したがって、このようなデジタル情報通信網上において音楽データや画像データ等の著作者の権利が存在するコンテンツが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【０００５】一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【０００６】ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したＣＤ（コンパクトディスク）については、ＣＤから光磁気ディスク（ＭＤ等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やＭＤ等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

【０００７】しかも、ＣＤからＭＤへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なＭＤからさらに他のＭＤに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【０００８】このような事情からも、音楽データや画像データ等のコンテンツデータをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【０００９】この場合、デジタル情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度、受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【００１０】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【００１１】最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化されたライセンスと、暗号化コンテンツデータをメモリカードに送信する。そして、メモリカードは、受信したライセンス鍵と暗号化コンテンツデータをメモリカードに記録する。

【００１２】そして、メモリカードに記録した暗号化コンテンツデータを再生するときは、メモリカードを携帯電話機に装着する。携帯電話機は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路を有する。

【００１３】各ユーザは、上述したように、自己の携帯電話機によって配信サーバから暗号化コンテンツデータおよびライセンスを受信し、その受信した暗号化コンテンツデータおよびライセンスを自己のメモリカードに記録する。

【００１４】

【発明が解決しようとする課題】しかし、各ユーザが新たに暗号化コンテンツデータを取得したいとき、その暗号化コンテンツデータが他のユーザのメモリカードに記録されている場合もある。そのような場合、各ユーザは、取得したい暗号化コンテンツデータを配信サーバから受信するのでは、暗号化コンテンツデータの受信に長時間を要し、かつ、通信費も高くなるという問題がある。

【００１５】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、ユーザが取得したい暗号化コンテンツデータの格納場所を検索し、その検索した格納場所から暗号化コンテンツデータを取得する情報端末装置を提供することである。

【００１６】

【課題を解決するための手段】この発明によれば、情報端末装置は、複数の情報端末装置において作成され、かつ、暗号化コンテンツデータを管理するための複数のベータベースを検索して暗号化コンテンツデータと暗号化コンテンツデータを再生するためのライセンスとを取得する情報端末装置であって、外部とのデータのやり取りを行なう送受信部と、指示を入力するためのキー操作部と、複数のデータベースと一覧表とを記憶する記憶部と、制御部とを備え、複数のデータベースの各々は、複

数の暗号化コンテンツデータを特定するための複数のコンテンツ特定情報と、暗号化コンテンツデータに対応するライセンスの有無を示す複数のライセンス情報と、暗号化コンテンツデータおよびライセンスが記録されたデータ記録装置を特定するための複数の記録装置特定情報とを含み、一覧表は、複数のベータベースを特定するための複数のデータベース特定情報と、複数のデータベースの各々が生成された情報端末装置を特定するための複数の端末特定情報とを含み、制御部は、暗号化コンテンツデータの購入要求に応じて、キー操作部を介して入力された購入コンテンツの検索条件を送受信部を介して配信サーバへ送信し、検索条件に合致するコンテンツのコンテンツ特定情報を配信サーバから送受信部を介して受信し、その受信したコンテンツ特定情報に一致するコンテンツ特定情報と一致したコンテンツ特定情報に対応するライセンス情報および端末特定情報とを複数のデータベースおよび一覧表から抽出し、その抽出したコンテンツ特定情報、ライセンス情報および端末特定情報を含む検索結果データベースを作成する。

【００１７】好ましくは、情報端末装置は、各種の情報を視覚情報としてユーザに与えるための表示部をさらに備え、制御部は、コンテンツ特定情報、ライセンス情報、および端末特定情報を検索結果データベースから読出して表示部に表示し、キー操作部を介して他の情報端末装置が保持する暗号化コンテンツデータの選択が入力されると、他の情報端末装置へ暗号化コンテンツデータの複製依頼を送受信部を介して送信し、他の情報端末装置において複製が許可されると他の情報端末装置から暗号化コンテンツデータを送受信部を介して受信する。

【００１８】好ましくは、制御部は、さらに、取得要求された暗号化コンテンツデータに対応するライセンス情報がライセンスの無しを表すとき、配信サーバから複製された暗号化コンテンツデータに対応するライセンスを受信する。

【００１９】好ましくは、情報端末装置は、各種の情報を視覚情報としてユーザに与えるための表示部と、データ記録装置との間のやり取りを制御するインタフェースとをさらに備え、制御部は、コンテンツ特定情報、ライセンス情報、および端末特定情報を前記検索結果データベースから読出して表示部に表示し、自己がやり取りを行なうデータ記録装置に記録された暗号化コンテンツデータの選択がキー操作部を介して入力され、選択された暗号化コンテンツデータに対応するライセンス情報がライセンスの無しを表すときライセンスの送信依頼を送受信部を介して配信サーバへ送信し、配信サーバから前記ライセンスを送受信部を介して受信する。

【００２０】好ましくは、情報端末装置は、各種の情報を視覚情報としてユーザに与えるための表示部と、データ記録装置との間のやり取りを制御するインタフェースとをさらに備え、制御部は、コンテンツ特定情報、ライセンス情報、および端末特定情報を検索結果データベースから読出して表示部に表示し、配信サーバが保持する暗号化コンテンツデータの選択がキー操作部を介して入力されたとき選択された暗号化コンテンツデータおよび選択された暗号化コンテンツデータに対応するライセンスの送信依頼を送受信部を介して配信サーバへ送信し、配信サーバから前記暗号化コンテンツデータおよびライセンスを前記送受信部を介して受信する。

【００２１】好ましくは、制御部は、さらに、データベースの取得要求に応じて他の情報端末装置が保持するデータベースを他の情報端末装置から送受信部を介して受信し、その受信したデータベースを記憶部に格納するとともに格納したデータベースを追加して一覧表を更新する。

【００２２】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【００２３】図１は、本発明による情報端末装置が暗号化コンテンツデータ、および暗号化コンテンツデータを復号するためのライセンスを取得するデータ配信システムの全体構成を概念的に説明するための概略図である。

【００２４】なお、以下では携帯電話網を介して音楽データをユーザの携帯電話機に装着されたメモリカード１１０～１１２に配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画像データ、ニュース、および英会話用のデータ等を配信する場合においても適用することが可能なものである。

【００２５】図１を参照して、配信キャリア２０は、自己の携帯電話網を通じて得た、ユーザからの配信要求（配信リクエスト）を配信サーバ１０に中継する。音楽データ等のコンテンツデータを管理する配信サーバ１０は、データ配信を求めてアクセスして来た携帯電話ユーザの携帯電話機１００（または１０１，１０２）に装着されたメモリカード１１０（または１１１，１１２）が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行ない、正当なメモリカードに対して著作権を保護するために所定の暗号方式によりコンテンツデータを暗号化した上で、データを配信するための配信キャリア２０である携帯電話会社に、このような暗号化コンテンツデータ、付加情報および暗号化コンテンツデータを再生するために必要な情報として暗号化コンテンツデータを復号するためのライセンス鍵を含むライセンスを与える。

【００２６】配信キャリア２０は、自己の携帯電話網を通じて配信要求を送信した携帯電話機１００（または１０１，１０２）に装着されたメモリカード１１０（また

は１１１，１１２）に対して、携帯電話網および携帯電話機１００（または１０１，０２）を介して暗号化コンテンツデータとライセンスとを配信する。

【００２７】図１においては、たとえば携帯電話ユーザの携帯電話機１００（または１０１，１０２）には、着脱可能なメモリカード１１０（または１１１，１１２）が装着される構成となっている。メモリカード１１０（または１１１，１１２）は、携帯電話機１００（または１０１，１０２）により受信された暗号化コンテンツデータを受取り、著作権を保護するために行なわれた暗号化を復号した上で、携帯電話機１００（または１０１，１０２）中の音楽再生部（図示せず）に与える。

【００２８】さらに、たとえば携帯電話ユーザは、携帯電話機１００（または１０１，１０２）に接続したヘッドホーン１３０（または１３１，１３２）等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

【００２９】このような構成とすることで、まず、メモリカード１１０（または１１１，１１２）を利用しないと、配信サーバ１０からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

【００３０】しかも、配信キャリア２０において、たとえば１曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア２０が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【００３１】したがって、図１に示すデータ配信システムにおいては、携帯電話機１００（または１０１，１０２）に装着されたメモリカード１１０（または１１１，１１２）は、携帯電話網を介して配信サーバ１０から暗号化コンテンツデータ、付加情報およびライセンスを受信して格納することができる。

【００３２】図１に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話機のユーザ側で再生可能とするためにシステム上必要とされるのは、第１には、通信におけるライセンスを配信するための方式であり、さらに第２には、コンテンツデータを暗号化する方式そのものであり、さらに、第３には、このようなコンテンツデータの無断コピーを防止するための著作権保護を実現する構成である。

【００３３】また、携帯電話機１００～１０２は、それぞれ、装着されたメモリカード１１０～１１２に格納された暗号化コンテンツデータを管理するためのデータベースを後述する方法によって作成し、その作成したベータベースを保持する。さらに、携帯電話機１００は、メモリカード１１１，１１２に格納された暗号化コンテンツデータを管理するためのデータベースを携帯電話機１０１，１０２から受信し、メモリカード１１０に格納された暗号化コンテンツデータを管理するためのデータベースとともに保持する。つまり、携帯電話機１００のユーザは、友人である携帯電話機１０１，１０２のユーザが所有するメモリカード１１１，１１２に格納された暗号化コンテンツデータを管理するためのデータベースを携帯電話機１０１，１０２から受信して保持する。このように、友人が配信サーバ１０から受信して自己のメモリカード１１１，１１２に格納した暗号化コンテンツデータを管理するためのデータベースを取得して携帯電話機１００に保持することによって、後述するように、携帯電話機１００のユーザは、新たな暗号化コンテンツデータを取得したいと思ったとき、その新たな暗号化コンテンツデータが既にメモリカード１１１，１１２へ配信されたものであれば、その新たな暗号化コンテンツデータを携帯電話機１０１，１０２を介してメモリカード１１１，１１２から取得できる。なお、携帯電話機１００と携帯電話機１０１，１０２との間の通信は、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉｅｓ　Ｂｕｓ）ケーブル６５を介して行なわれてもよく、無線通信によって行なわれてもよい。

【００３４】そして、携帯電話機１００は、携帯電話機１０１，１０２から受信した暗号化コンテンツデータを復号および再生するためのライセンスを携帯電話網を介して配信サーバ１０から受信する。配信サーバ１０は、ライセンスの配信に対して課金を行なうので、ライセンスの取得は原則として配信サーバ１０から行なうこととしたものである。

【００３５】本発明の実施の形態においては、特に、配信、および再生の各処理の発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証の記録装置および情報端末装置（暗号化コンテンツデータを復号して再生できる再生端末を携帯電話機とも言う。以下同じ）に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【００３６】なお、以下の説明においては、配信サーバ１０から、各携帯電話機に暗号化コンテンツデータ、付加情報、およびライセンスを伝送する処理を「配信」と称することとする。

【００３７】図２は、図１に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【００３８】まず、配信サーバ１０より配信されるデータについて説明する。Ｄｃは、音楽データ等のコンテンツデータである。コンテンツデータＤｃは、ライセンス鍵Ｋｃで復号可能な暗号化が施される。ライセンス鍵Ｋｃによって復号可能な暗号化が施された暗号化コンテンツデータ｛Ｄｃ｝Ｋｃがこの形式で配信サーバ１０より携帯電話機のユーザに配布される。

【００３９】なお、以下においては、｛Ｙ｝Ｘという表

記は、データＹを、復号鍵Ｘにより復号可能な暗号化を施したことを示すものとする。

【００４０】さらに、配信サーバ１０からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Ｄｃ－ｉｎｆが配布される。

【００４１】また、ライセンスとして、ライセンス鍵Ｋｃと、配信サーバ１０からのライセンス鍵等の配信を特定するための管理コードであるライセンスＩＤとが配信サーバ１０と携帯電話機１００（または１０１，１０２）との間でやり取りされる。さらに、ライセンスとしては、コンテンツデータＤｃを識別するためのコードであるコンテンツＩＤや、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ＡＣに基づいて生成される、記録装置（メモリカード）におけるライセンスのアクセスに対する制限に関する情報であるアクセス制御情報ＡＣｍおよび情報端末装置における再生に関する制御情報である再生制御情報ＡＣｐ等が存在する。具体的には、アクセス制御情報ＡＣｍは、メモリカードからのライセンスまたはライセンス鍵を外部に出力するに当っての制御情報であり、再生可能回数（再生のためにライセンス鍵を出力する数）、ライセンスの移動・複製に関する制限情報などがある。再生制御情報ＡＣｐは、コンテンツデータを再生するためにコンテンツ再生回路がライセンス鍵を受取った後に、再生を制限する情報であり、再生期限、再生速度変更制限、再生範囲指定（部分ライセンス）などがある。

【００４２】以後、ライセンスＩＤと、コンテンツＩＤと、ライセンス鍵Ｋｃと、アクセス制御情報ＡＣｍと、再生制御情報ＡＣｐとを併せて、ライセンスと総称することとする。

【００４３】図３は、図１に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を説明する図である。

【００４４】情報端末装置内のコンテンツ再生デバイス、およびメモリカードには固有の公開暗号鍵ＫＰｐｙおよびＫＰｍｗがそれぞれ設けられ、公開暗号鍵ＫＰｐｙおよびＫＰｍｗは、コンテンツ再生デバイスに固有の秘密復号鍵Ｋｐｙ、メモリカードに固有の秘密復号鍵Ｋｍｗによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、メモリカードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称し、これらの公開暗号鍵をクラス公開暗号鍵、秘密復号鍵をクラス秘密復号鍵、クラス鍵を共有する単位をクラスと称する。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

【００４５】また、コンテンツ再生デバイスのクラス証明書としてＣｐｙが設けられ、メモリカードのクラス証明書としてＣｍｗが設けられる。これらのクラス証明書は、コンテンツ再生デバイス、およびメモリカードのクラスごとに異なる情報を有する。

【００４６】これらのコンテンツ再生デバイスのクラス公開暗号鍵およびクラス証明書は、認証データ｛ＫＰｐｙ／／Ｃｐｙ｝ＫＰａの形式で、メモリカードのクラス公開暗号鍵およびクラス証明書は、認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａの形式で出荷時にデータ再生デバイス、およびメモリカードにそれぞれ記録される。後ほど詳細に説明するが、ＫＰａは配信システム全体で共通の公開認証鍵である。

【００４７】また、メモリカード１１０内のデータ処理を管理するための鍵として、メモリカードという媒体ごとに設定される公開暗号鍵ＫＰｍｃｘと、公開暗号鍵ＫＰｍｃｘで暗号化されたデータを復号することが可能なそれぞれに固有の秘密復号鍵Ｋｍｃｘが存在する。これらのメモリカードごとに設定される公開暗号鍵および秘密復号鍵を総称して個別鍵と称し、公開暗号鍵ＫＰｍｃｘを個別公開暗号鍵、秘密復号鍵Ｋｍｃｘを個別秘密復号鍵と称する。

【００４８】ライセンスの配信、および再生が行なわれるごとに配信サーバ１０、携帯電話機１００～１０２、およびメモリカード１１０～１１２において生成される共通鍵Ｋｓ１～Ｋｓ３が用いられる。

【００４９】ここで、共通鍵Ｋｓ１～Ｋｓ３は、配信サーバ、コンテンツ再生デバイスもしくはメモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ｋｓ１～Ｋｓ３を「セッションキー」とも呼ぶこととする。

【００５０】これらのセッションキーＫｓ１～Ｋｓ３は、各セッションごとに固有の値を有することにより、配信サーバ、コンテンツ再生デバイス、およびメモリカードによって管理される。具体的には、セッションキーＫｓ１は、配信サーバによって配信セッションごとに発生される。セッションキーＫｓ２は、メモリカードによって配信セッションおよび再生セッションごとに発生し、セッションキーＫｓ３は、コンテンツ再生デバイスにおいて再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行した上でライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【００５１】図４は、図１に示した配信サーバ１０の構成を示す概略ブロック図である。配信サーバ１０は、コンテンツデータを所定の方式に従って暗号化したデータやコンテンツＩＤ等の配信情報を保持するための情報データベース３０４と、携帯電話機の各ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース３０２と、情報データベー

ス３０４に保持されたコンテンツデータのメニューを保持するメニューデータベース３０７と、ライセンスの配信ごとに生成され、かつ、ライセンスを特定するライセンスＩＤ等の配信に関するログを保持する配信記録データベース３０８と、情報データベース３０４、課金データベース３０２、メニューデータベース３０７、および配信記録データベース３０８からのデータをバスＢＳ１を介して受取り、所定の処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

【００５２】データ処理部３１０は、バスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１５と、配信制御部３１５に制御されて、配信セッション時にセッションキーＫｓ１を発生するためのセッションキー発生部３１６と、メモリカードから送られてきた認証のための認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａを復号するための公開認証鍵ＫＰａを保持する認証鍵保持部３１３と、メモリカードから送られてきた認証のための認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａを通信装置３５０およびバスＢＳ１を介して受けて、認証鍵保持部３１３からの公開認証鍵ＫＰａによって復号処理を行なう復号処理部３１２と、配信セッションごとに、セッションキーＫｓ１を発生するセッションキー発生部３１６と、セッションキー発生部３１６により生成されたセッションキーＫｓ１を復号処理部３１２によって得られたクラス公開暗号鍵ＫＰｍｗを用いて暗号化して、バスＢＳ１に出力するための暗号処理部３１８と、セッションキーＫｓ１によって暗号化された上で送信されたデータをバスＢＳ１より受けて、復号処理を行なう復号処理部３２０とを含む。

【００５３】データ処理部３１０は、さらに、配信制御部３１５から与えられるライセンス鍵Ｋｃおよびアクセス制御情報ＡＣｍを、復号処理部３２０によって得られたメモリカードごとに個別公開暗号鍵ＫＰｍｃｘによって暗号化するための暗号処理部３２６と、暗号処理部３２６の出力を、復号処理部３２０から与えられるセッションキーＫｓ２によってさらに暗号化してバスＢＳ１に出力するための暗号処理部３２８とを含む。

【００５４】配信サーバ１０の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【００５５】図５は、図１に示した携帯電話機１００～１０２の構成を説明するための概略ブロック図である。

【００５６】携帯電話機１００～１０２は、携帯電話機１００～１０２の各部のデータ授受を行なうためのバスＢＳ２と、携帯電話網により無線伝送される信号を受信するためのアンテナ１１０１と、アンテナ１１０１からの信号を受けてベースバンド信号に変換し、あるいは携帯電話機１００～１０２の各部からのデータを変調してアンテナ１１０１に与えるための送受信部１１０２とを含む。

【００５７】携帯電話機１００～１０２は、さらに、暗号化コンテンツデータとともにメモリカード１１０～１１２に格納されたコンテンツ管理情報に基づいて作成された、暗号化コンテンツデータを管理するためのデータベースを格納するＲＡＭ１１０３を含む。なお、ＲＡＭ１１０３は、他の携帯電話機から取得したデータベースも格納する。

【００５８】携帯電話機１００～１０２は、さらに、バスＢＳ２を介して携帯電話機１００～１０２の動作を制御するためのコントローラ１１０６と、外部からの指示を携帯電話機１００～１０２に与えるためのキー操作部１１０８と、コントローラ１１０６等から出力される情報をユーザに視覚情報として与えるための表示パネル１１１０とを含む。

【００５９】携帯電話機１００～１０２は、さらに、配信サーバ１０または他の携帯電話機からのコンテンツデータ（音楽データ）を記憶し、かつ、復号処理を行なうための着脱可能なメモリカード１１０～１１２と、メモリカード１１０～１１２とバスＢＳ２との間のデータの授受を制御するためのメモリカードインタフェース１２００とを含む。

【００６０】携帯電話機１００～１１２は、さらに、クラス公開暗号鍵ＫＰｐ１およびクラス証明書Ｃｐ１を公開認証鍵ＫＰａで復号することでその正当性を認証できる状態に暗号化した認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを保持する認証データ保持部１５００を含む。ここで、携帯電話機１００～１０２のクラスｙは、ｙ＝１であるとする。

【００６１】携帯電話機１００～１０２は、さらに、クラス固有の復号鍵であるＫｐ１を保持するＫｐ１保持部１５０２と、バスＢＳ２から受けたデータをＫｐ１によって復号し、メモリカード１１０～１１２によって発生されたセッションキーＫｓ２を得る復号処理部１５０４とを含む。

【００６２】携帯電話機１００～１０２は、さらに、メモリカード１１０～１１２に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード１１０～１１２との間でバスＢＳ２上においてやり取りされるデータを暗号化するためのセッションキーＫｓ３を乱数等により発生するセッションキー発生部１５０８と、暗号化コンテンツデータの再生セッションにおいてメモリカード１１０～１１２からライセンス鍵Ｋｃおよび再生制御情報ＡＣｐを受取る際に、セッションキー発生部１５０８により発生されたセッションキーＫｓ３を復号処理部１５０４によって得られたセッションキーＫｓ２によって暗号化し、バスＢＳ２に出力する暗号処理部１５０６とを含む。

【００６３】携帯電話機１００～１０２は、さらに、バ

スＢＳ２上のデータをセッションキーＫｓ３によって復号して、ライセンス鍵Ｋｃおよび再生制御情報ＡＣｐを出力する復号処理部１５１０と、バスＢＳ２より暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを受けて、復号処理部１５１０からのライセンス鍵Ｋｃによって暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを復号してコンテンツデータＤｃを音楽再生部１５１８へ出力する復号処理部１５１６とを含む。

【００６４】携帯電話機１００～１０２は、さらに、復号処理部１５１６からの出力を受けてコンテンツデータを再生するための音楽再生部１５１８と、音楽再生部１５１８の出力をディジタル信号からアナログ信号に変換するＤＡ変換器１５１９と、ＤＡ変換器１５１９の出力をヘッドホーンなどの外部出力装置（図示省略）へ出力するための端子１５３０とを含む。

【００６５】携帯電話機１００～１０２は、さらに、他の携帯電話機からコンテンツデータ、付加情報およびライセンスを受信する際にバスＢＳ２と端子１１１４との間のデータ授受を制御するためのＵＳＢインタフェース１１１２と、ＵＳＢケーブル６５を接続するための端子１１１４とを含む。

【００６６】また、図５においては、点線で囲んだ領域は暗号化コンテンツデータを復号して音楽データを再生するコンテンツ再生デバイス１５５０を構成する。

【００６７】さらに、図５においては、通常の通話機能に必要な音声データの変調および復号を行なう音声コーデック、およびマイク等は省略している。

【００６８】携帯電話機１００～１０２の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【００６９】図６は、図１に示すメモリカード１１０～１１２の構成を説明するための概略ブロック図である。

【００７０】既に説明したように、メモリカードのクラス公開暗号鍵およびクラス秘密復号鍵として、ＫＰｍｗおよびＫｍｗが設けられ、メモリカードのクラス証明書Ｃｍｗが設けられるが、メモリカード１１０においては、自然数ｗ＝３で表わされるものとする。また、メモリカードを識別する自然数ｘは、メモリカード１１０に対してはｘ＝４で表わされるものとする。

【００７１】したがって、メモリカード１１０は、認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを保持する認証データ保持部１４００と、メモリカードごとに設定される固有の復号鍵である個別秘密復号鍵Ｋｍｃ４を保持するＫｍｃ保持部１４０２と、クラス秘密復号鍵Ｋｍ３を保持するＫｍ保持部１４２１と、個別秘密復号鍵Ｋｍｃ４によって復号可能な公開暗号鍵ＫＰｍｃ４を保持するＫＰｍｃ保持部１４１６とを含む。

【００７２】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【００７３】メモリカード１１０は、さらに、メモリカードインタフェース１２００との間で信号を端子１４２６を介して授受するインタフェース１４２４と、インタフェース１４２４との間で信号をやり取りするバスＢＳ３と、バスＢＳ３にインタフェース１４２４から与えられるデータから、クラス秘密復号鍵Ｋｍ３をＫｍ保持部１４２１から受けて、配信サーバ１０が配信セッションにおいて生成したセッションキーＫｓ1を接点Ｐａに出力する復号処理部１４２２と、ＫＰａ保持部１４１４から公開認証鍵ＫＰａを受けて、バスＢＳ３に与えられるデータの公開認証鍵ＫＰａによる復号処理を実行して復号結果と得られたクラス証明書をコントローラ１４２０に、得られたクラス公開鍵を暗号処理部１４１０に出力する復号処理部１４０８と、切換スイッチ１４４２によって選択的に与えられる鍵によって、切換スイッチ１４４６によって選択的に与えられるデータを暗号化してバスＢＳ４に出力する暗号処理部１４０６とを含む。

【００７４】メモリカード１１０は、さらに、配信、および再生の各セッションにおいてセッションキーＫｓ２を発生するセッションキー発生部１４１８と、セッションキー発生部１４１８の出力したセッションキーＫｓ２を復号処理部１４０８によって得られるクラス公開暗号鍵ＫＰｐｙもしくはＫＰｍｗによって暗号化してバスＢＳ３に出力する暗号処理部１４１０と、バスＢＳ３よりセッションキーＫｓ２によって暗号化されたデータを受けてセッションキー発生部１４１８より得たセッションキーＫｓ２によって復号する復号処理部１４１２と、暗号化コンテンツデータの再生セッションにおいてメモリ１４１５から読出されたライセンス鍵Ｋｃおよび再生制御情報ＡＣｐを、復号処理部１４１２で復号された他のメモリカード１１０の個別公開暗号鍵ＫＰｍｃｘ（ｘ≠４）で暗号化する暗号処理部１４１７とを含む。

【００７５】メモリカード１１０は、さらに、バスＢＳ３上のデータを個別公開暗号鍵ＫＰｍｃ４と対をなすメモリカード１１０の個別秘密復号鍵Ｋｍｃ４によって復号するための復号処理部１４０４と、配信サーバ１０との間の通信における履歴を格納するログと、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを再生するためのライセンス（Ｋｃ，ＡＣｐ，ＡＣｍ，ライセンスＩＤ，コンテンツＩＤ）と、付加情報Ｄｃ－ｉｎｆと、暗号化コンテンツデータの再生リストと、ライセンスを管理するためのライセンス管理ファイルとをバスＢＳ３より受けて格納するためのメモリ１４１５とを含む。メモリ１４１５は、例えば半導体メモリによって構成される。また、メモリ１４１５は、ログ領域１４１５Ａと、ライセンス領域１４１５Ｂと、データ領域１４１５Ｃとから成る。ログ領域１４１５Ａは、ログを記録するための領域である。ログ領域１４１

５Ａは、メモリカード１１０に対してライセンスが入力され、格納されるときに記録される受信ログを含む。

【００７６】ライセンス領域１４１５Ｂは、ライセンスを記録するための領域である。ライセンス領域１４１５Ｂは、ライセンス（ライセンス鍵Ｋｃ、再生制御情報ＡＣｐ、アクセス制限情報ＡＣｍ、ライセンスＩＤ、コンテンツＩＤ）を格納する。ライセンスは、エントリ番号に対応してライセンス領域１４１５Ｂに格納されており、ライセンスに対してアクセスする場合には、ライセンスが格納されている、あるいは、ライセンスを記録したいエントリをエントリ番号によって指定する構成になっている。

【００７７】データ領域１４１５Ｃは、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃ、暗号化コンテンツデータの付加情報Ｄｃ－ｉｎｆ、ライセンスを管理するために必要な情報を暗号化コンテンツごとに記録するライセンス管理ファイル、およびメモリカードに記録された暗号化コンテンツデータやライセンスにアクセスするための基本的な情報を記録する再生リストを記録するための領域である。そして、データ領域１４１５Ｃは、外部から直接アクセスすることができる。

【００７８】メモリカード１１０は、さらに、バスＢＳ３を介して外部との間でデータ授受を行ない、バスＢＳ３との間で再生情報等を受けて、メモリカード１１０の動作を制御するためのコントローラ１４２０を含む。

【００７９】なお、データ領域１４１５Ｃを除く全ての構成は、耐タンパモジュール領域に構成される。

【００８０】また、メモリカード１１１，１１２は、メモリカード１１０と同じ構成からなる。この場合、メモリカードを識別するための自然数ｘは、「４」以外の自然数が用いられる。

【００８１】以下、図１に示すデータ配信システムにおける各セッションの動作について説明する。

【００８２】［配信］まず、図１に示すデータ配信システムにおいて、配信サーバ１０から携帯電話機１００のメモリカード１１０へ暗号化コンテンツデータおよびライセンスを配信する動作について説明する。

【００８３】図７および図８は、図１に示すデータ配信システムにおける暗号化コンテンツデータの購入時に発生する携帯電話機１００に装着されたメモリカード１１０への暗号化コンテンツデータ｛Ｄｃ｝Ｋｃ、付加情報Ｄｃ－ｉｎｆ、およびライセンスの配信動作（以下、配信セッションともいう）を説明するための第１および第２のフローチャートである。

【００８４】図７における処理以前に、携帯電話機１００のユーザは、配信サーバ１０に対して携帯電話網を介して接続し、購入を希望するコンテンツに対するコンテンツＩＤを取得していることを前提としている。

【００８５】図７を参照して、携帯電話機１００のユーザからキー操作部１１０８を介してコンテンツＩＤの指定による配信リクエストがなされる（ステップＳ１００）。そして、キー操作部１１０８を介して暗号化コンテンツデータのライセンスを購入するための購入条件ＡＣを入力するように指示し、購入条件ＡＣが入力される（ステップＳ１０２）。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵Ｋｃを購入するために、暗号化コンテンツデータのアクセス制御情報ＡＣｍ、および再生制御情報ＡＣｐを設定して購入条件ＡＣが入力される。

【００８６】暗号化コンテンツデータの購入条件ＡＣが入力されると、コントローラ１１０６は、バスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード１１０へ認証データの出力指示を与える（ステップＳ１０４）。メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介して認証データの送信要求を受信する（ステップＳ１０６）。そして、コントローラ１４２０は、バスＢＳ３を介して認証データ保持部１４００から認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを読出し、｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ３、インタフェース１４２４および端子１４２６を介して出力する（ステップＳ１０８）。

【００８７】携帯電話機１００のコントローラ１１０６は、メモリカード１１０からの認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａに加えて、コンテンツＩＤ、ライセンス購入条件のデータＡＣ、および配信リクエストを配信サーバ１０に対して送信する（ステップＳ１１０）。

【００８８】配信サーバ１０では、携帯電話機１００から配信リクエスト、コンテンツＩＤ、認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ、およびライセンス購入条件のデータＡＣを受信し（ステップＳ１１２）、復号処理部３１２においてメモリカード１１０から出力された認証データを公開認証鍵ＫＰａで復号処理を実行する（ステップＳ１１４）。

【００８９】配信制御部３１５は、復号処理部３１２における復号処理結果から、正規の機関でその正当性を証明するための暗号化を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ１１６）。正当な認証データであると判断された場合、配信制御部３１５は、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を承認し、受理する。そして、次の処理（ステップＳ１１８）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を受理しないで配信セッションを終了する（ステップＳ１８４）。

【００９０】認証の結果、正当な認証データを持つメモリカードを装着した携帯電話機からのアクセスであることが確認されると、配信サーバ１０において、セッションキー発生部３１６は、配信のためのセッションキーＫｓ１を生成する（ステップＳ１１８）。セッションキー

Ｋｓ１は、復号処理部３１２によって得られたメモリカード１１０に対応するクラス公開暗号鍵ＫＰｍ３によって、暗号処理部３１８によって暗号化される（ステップＳ１２０）。

【００９１】配信制御部３１５は、ライセンスＩＤを生成し（ステップＳ１２２）、ライセンスＩＤおよび暗号化されたセッションキーＫｓ１は、ライセンスＩＤ／／｛Ｋｓ１｝Ｋｍ３として、バスＢＳ１および通信装置３５０を介して外部に出力される（ステップＳ１２４）。

【００９２】携帯電話機１００が、ライセンスＩＤ／／｛Ｋｓ１｝Ｋｍ３を受信すると、コントローラ１１０６は、ライセンスＩＤ／／｛Ｋｓ１｝Ｋｍ３をメモリカード１１０に入力する（ステップＳ１２６）。そうすると、メモリカード１１０においては、端子１４２６およびインタフェース１４２４を介して、コントローラ１４２０は、ライセンスＩＤ／／｛Ｋｓ１｝Ｋｍ３を受理する（ステップＳ１２８）。そして、コントローラ１４２０は、バスＢＳ３を介してメモリ１４１５のログ領域１４１５Ａに記録されている受信ログを初期化し、受理したライセンスＩＤをログ領域１４１５Ａに格納する（ステップＳ１３０）。このとき、受信ログ内の受信ｓｔａｔｅは、ＯＦＦに設定される。その後、コントローラ１４２０は、バスＢＳ３を介して｛Ｋｓ１｝Ｋｍ３を復号処理部１４２２に与え、復号処理部１４２２は、Ｋｍ保持部１４２１に保持されるメモリカード１１０に固有なクラス秘密復号鍵Ｋｍ３によって｛Ｋｓ１｝Ｋｍ３を復号処理することにより、セッションキーＫｓ１を復号し、セッションキーＫｓ１を受理する（ステップＳ１３２）。

【００９３】コントローラ１４２０は、配信サーバ１０で生成されたセッションキーＫｓ１の受理を確認すると、セッションキー発生部１４１８に対してメモリカード１１０において配信動作時に生成されるセッションキーＫｓ２の生成を指示する。そして、セッションキー発生部１４１８は、セッションキーＫｓ２を生成する（ステップＳ１３４）。コントローラ１４２０は、生成されたセッションキーＫｓ２をバスＢＳ３を介して受取り、その受取ったセッションキーＫｓ２をメモリ１４１５のログ領域１４１５Ａに格納し、受信ｓｔａｔｅをＯＮにする（ステップＳ１３６）。

【００９４】暗号処理部１４０６は、切換スイッチ１４４２の接点Ｐａを介して復号処理部１４２２より与えられるセッションキーＫｓ１によって、切換スイッチ１４４６の接点を順次切換えることによって与えられるセッションキーＫｓ２、および個別公開暗号鍵ＫＰｍｃ４を１つのデータ列として暗号化して、｛Ｋｓ２／／ＫＰｍｃ４｝Ｋｓ１をバスＢＳ３に出力する。バスＢＳ３に出力された暗号化データ｛Ｋｓ２／／ＫＰｍｃ４｝Ｋｓ１は、バスＢＳ３からインタフェース１４２４および端子１４２６を介して携帯電話機１００に出力され（ステップＳ１３８）、携帯電話機１００から配信サーバ１０に送信される（ステップＳ１４０）。

【００９５】図８を参照して、配信サーバ１０は、｛Ｋｓ２／／ＫＰｍｃ４｝Ｋｓ１を受信して、復号処理部３２０においてセッションキーＫｓ１による復号処理を実行し、メモリカード１１０で生成されたセッションキーＫｓ２、およびメモリカード１１０の個別公開暗号鍵ＫＰｍｃ４を受理する（ステップＳ１４２）。

【００９６】配信制御部３１５は、ステップＳ１１２で取得したコンテンツＩＤに従ってライセンス鍵Ｋｃを情報データベース３０４から取得し（ステップＳ１４４）、ステップＳ１１２で取得したライセンス購入条件のデータＡＣに従って、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐを決定する（ステップＳ１４６）。

【００９７】配信制御部３１５は、生成したライセンス、すなわち、ライセンスＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、再生制御情報ＡＣｐ、およびアクセス制御情報ＡＣｍを暗号処理部３２６に与える。暗号処理部３２６は、復号処理部３２０によって得られたメモリカード１１０の個別公開暗号鍵ＫＰｍｃ４によってライセンスを暗号化して暗号化データ｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を生成する（ステップＳ１４８）。そして、暗号処理部３２８は、暗号処理部３２６からの暗号化データ｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を、復号処理部３２０からのセッションキーＫｓ２によって暗号化し、暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を出力する。配信制御部３１５は、バスＢＳ１および通信装置３５０を介して暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を携帯電話機１００へ送信する（ステップＳ１５０）。

【００９８】携帯電話機１００は、送信された暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信し、バスＢＳ２を介してメモリカード１１０に入力する（ステップＳ１５２）。メモリカード１１０においては、端子１４２６およびインタフェース１４２４を介して、バスＢＳ３に与えられた受信データを復号処理部１４１２によって復号する。復号処理部１４１２は、セッションキー発生部１４１８から与えられたセッションキーＫｓ２を用いてバスＢＳ３上の受信データを復号し、バスＢＳ３に出力する（ステップＳ１５４）。

【００９９】この段階で、バスＢＳ３には、Ｋｍｃ保持部１４０２に保持される個別秘密復号鍵Ｋｍｃ４で復号可能な暗号化ライセンス｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４が出力される（ステップＳ１５４）。

【０１００】コントローラ１４２０の指示によって、暗

号化ライセンス｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４は、復号処理部１４０４において、個別秘密復号鍵Ｋｍｃ４によって復号され、ライセンス（ライセンス鍵Ｋｃ、ライセンスＩＤ、コンテンツＩＤ、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐ）が受理される（ステップＳ１５６）。そして、この段階で携帯電話機１００のコントローラ１１０６から端子１４２６およびインタフェース１４２４を介してライセンスを格納するためのエントリ番号が入力される。

【０１０１】そうすると、コントローラ１４２０は、受理したライセンス（ライセンス鍵Ｋｃ、ライセンスＩＤ、コンテンツＩＤ、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐ）を受理したエントリ番号に従ってメモリ１４１５のライセンス領域１４１５Ｂに格納する（ステップＳ１５８）。そして、コントローラ１４２０は、バスＢＳ３を介してメモリ１４１５のログ領域１４１５Ａの受信ログに記録された受信ｓｔａｔｅをＯＦＦする（ステップＳ１６０）。ライセンスの書込みが終了すると、携帯電話機１００のコントローラ１１０６は、ライセンス管理情報を更新し、その更新したライセンス管理情報をメモリカード１１０へ入力する（ステップＳ１６２）。メモリカード１１０のコントローラ１４２０は、入力されたライセンス管理情報をメモリ１４１５のデータ領域１４１５Ｃに書込む（ステップＳ１６４）。

【０１０２】ライセンスの配信が終了した後、携帯電話機１００のコントローラ１１０６は、暗号化コンテンツデータの配信要求を配信サーバ１０へ送信し（ステップＳ１６６）、配信サーバ１０は、暗号化コンテンツデータの配信要求を受信する（ステップＳ１６８）。そして、配信サーバ１０の配信制御部３１５は、情報データベース３０４より、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを取得して、これらのデータをバスＢＳ１および通信装置３５０を介して出力する（ステップＳ１７０）。

【０１０３】携帯電話機１００は、｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆを受信して、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを受理する（ステップＳ１７２）。そうすると、コントローラ１１０６は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆをバスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード１１０に入力する（ステップＳ１７４）。

【０１０４】メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを受理し、その受理した暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆをメモリ１４１５のデータ領域１４１５Ｃに記録する（ステップＳ１７６）。そして、コントローラ１４２０は、受理したコンテンツの情報をデータ領域１４１５Ｃの再生リストに追記する（ステップＳ１７８）。

【０１０５】そうすると、携帯電話機１００のコントローラ１１０６は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆの配信受理を配信サーバ１０へ送信し（ステップＳ１８０）、配信サーバ１０は、配信受理を受信し、配信制御部３１５は、バスＢＳ１を介して課金データベース３０２に書込んで課金処理を行なう（ステップＳ１８２）。そして、配信動作が終了する（ステップＳ１８４）。

【０１０６】このようにして、携帯電話機１００に装着されたメモリカード１１０が正規の認証データを保持する機器であること、同時に、クラス証明書Ｃｍ３とともに暗号化して送信できた公開暗号鍵ＫＰｍ３が有効であることを確認した上でコンテンツデータを配信することができ、不正なメモリカードへのコンテンツデータの配信を禁止することができる。

【０１０７】また、携帯電話機１０１，１０２に装着されたメモリカード１１１，１１２への暗号化コンテンツデータ、付加情報、およびライセンスの配信も図７および図８に示すフローチャートに従って行なわれる。

【０１０８】図９は、メモリカード１１０のメモリ１４１５におけるライセンス領域１４１５Ｂとデータ領域１４１５Ｃとを示したものである。データ領域１４１５Ｃには、再生リストファイル１６０と、エントリ管理情報１６５と、カードＩＤ１６６と、コンテンツファイル１６１１～１６１ｎと、ライセンス管理ファイル１６２１～１６２ｎとが記録されている。コンテンツファイル１６１１～１６１ｎは、受信した暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとを１つのファイルとして記録する。また、ライセンス管理ファイル１６２１～１６２ｎは、それぞれ、コンテンツファイル１６１１～１６１ｎに対応して記録され、対応するコンテンツファイル１６１１～１６１ｎに記録された暗号化コンテンツデータを復号および再生するためのライセンスが格納されたエントリ番号を含む。

【０１０９】ライセンス領域１４１５Ｂは、エントリ番号によって指定された領域にライセンスと有効フラグとを格納する。したがって、ライセンス管理ファイル１６２１～１６２ｎからエントリ番号を読出せば、その読出したエントリ番号によってライセンス管理ファイル１６２１～１６２ｎに対応するコンテンツファイル１６１１～１６１ｎに記録された暗号化コンテンツデータを復号するためのライセンスをライセンス領域１４１５Ｂから読出すことができる構成になっている。また、有効フラグは、ライセンスをメモリカード１１０から外部へ出すことができるか否かを示すものであり、メモリカード１１０にライセンスが格納されているときは「有効」と記録され、後述するライセンスの移動によってライセンスをメモリカード１１０から外部へ出したときは「無効」

と記録される。

【０１１０】メモリカード１１０は、配信サーバ１０から暗号化コンテンツデータおよびライセンスを受信したとき、暗号化コンテンツデータおよびライセンスをメモリ１４１５に記録する。

【０１１１】また、ライセンス管理ファイル１６２２は、点線で示されているが、実際には記録されていないことを示す。コンテンツファイル１６１２は存在しているがライセンスが無く再生できないことを表しているが、これは、たとえば、携帯電話機が他の携帯電話機から暗号化コンテンツデータだけを受信した場合に相当する。

【０１１２】図１０は、図９に示すコンテンツファイル１６１１～１６１ｎに記録された暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとの関係を示す概念図である。なお、図１０は、コンテンツ数が１０個の場合を示す。コンテンツデータ１６３１～１６４０は、それぞれ、コンテンツファイル１６１１～１６２０に記録された暗号化コンテンツデータである。コンテンツ管理情報１６３は、管理情報１６５１～１６６０から成り、管理情報１６５１～１６６０は、コンテンツＩＤ、タイトル名、アーティスト名およびコンテンツ種別を含む。そして、管理情報１６５１～１６６０は、それぞれ、コンテンツデータ１６３１～１６４０を管理するための管理情報である。したがって、管理情報１６５１～１６６０は、それぞれ、コンテンツデータ１６３１～１６４０に対応付けられてコンテンツ管理情報１６３を構成する。

【０１１３】［再生］携帯電話機１００に装着されたメモリカード１１０が、配信サーバ１０から受信した暗号化コンテンツデータの再生動作について説明する。

【０１１４】図１１は、メモリカード１１０が受信したコンテンツデータの携帯電話機１００における再生動作を説明するためのフローチャートである。なお、図１１における処理以前に、携帯電話機１００のユーザは、メモリカード１００のデータ領域１４１５Ｃに記録されている再生リストに従って、再生するコンテンツ（楽曲）を決定し、コンテンツファイルを特定し、ライセンス管理ファイルを取得していることを前提としている。

【０１１５】図１１を参照して、再生動作の開始とともに、携帯電話機１００のユーザからキー操作部１１０８を介して再生リクエストが携帯電話機１００にインプットされる（ステップＳ７００）。そうすると、コントローラ１１０６は、バスＢＳ２を介して認証データの出力要求をコンテンツ再生デバイス１５５０に行ない（ステップＳ７０２）、コンテンツ再生デバイス１５５０は認証データの出力要求を受信する（ステップＳ７０４）。そして、認証データ保持部１５００は、認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを出力し（ステップＳ７０６）、コントローラ１１０６は、メモリカードインタフェース１２００を介してメモリカード１１０へ認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを入力する（ステップＳ７０８）。

【０１１６】そうすると、メモリカード１１０は、認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを受理し、復号処理部１４０８は、受理した認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを、ＫＰａ保持部１４１４に保持された公開認証鍵ＫＰａによって復号し（ステップＳ７１０）、コントローラ１４２０は復号処理部１４０８における復号処理結果から、認証処理を行なう。すなわち、認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａが正規の認証データであるか否かを判断する認証処理を行なう（ステップＳ７１２）。復号できなかった場合、ステップＳ７４６へ移行し、再生動作は終了する。認証データが復号できた場合、コントローラ１４２０は、セッションキー発生部１４１８を制御し、セッションキー発生部１４１８は、再生セッション用のセッションキーＫｓ２を発生させる（ステップＳ７１３）。そして、暗号処理部１４１０は、セッションキー発生部１４１８からのセッションキーＫｓ２を、復号処理部１４０８で復号された公開暗号鍵ＫＰｐ１によって暗号化した｛Ｋｓ２｝Ｋｐ１をバスＢＳ３へ出力する。そうすると、コントローラ１４２０は、インタフェース１４２４および端子１４２６を介してメモリカードインタフェース１２００へ｛Ｋｓ２｝Ｋｐ１を出力する（ステップＳ７１４）。携帯電話機１００のコントローラ１１０６は、メモリカードインタフェース１２００を介して｛Ｋｓ２｝Ｋｐ１を取得する。そして、コントローラ１１０６は、｛Ｋｓ２｝Ｋｐ１をバスＢＳ２を介してコンテンツ再生デバイス１５５０の復号処理部１５０４へ与え（ステップＳ７１６）、復号処理部１５０４は、Ｋｐ１保持部１５０２から出力された、公開暗号鍵ＫＰｐ１と対になっている秘密復号鍵Ｋｐ１によって｛Ｋｓ２｝Ｋｐ１を復号し、セッションキーＫｓ２を暗号処理部１５０６へ出力する（ステップＳ７１８）。そうすると、セッションキー発生部１５０８は、再生セッション用のセッションキーＫｓ３を発生させ、セッションキーＫｓ３を暗号処理部１５０６へ出力する（ステップＳ７２０）。暗号処理部１５０６は、セッションキー発生部１５０８からのセッションキーＫｓ３を復号処理部１５０４からのセッションキーＫｓ２によって暗号化して｛Ｋｓ３｝Ｋｓ２を出力し（ステップＳ７２２）、コントローラ１１０６は、バスＢＳ２およびメモリカードインタフェース１２００を介して｛Ｋｓ３｝Ｋｓ２をメモリカード１１０へ出力する（ステップＳ７２４）。

【０１１７】そうすると、メモリカード１１０の復号処理部１４１２は、端子１４２６、インタフェース１４２４、およびバスＢＳ３を介して｛Ｋｓ３｝Ｋｓ２を入力する。復号処理部１４１２は、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によっ

て｛Ｋｓ３｝Ｋｓ２を復号して、携帯電話機１００で発生されたセッションキーＫｓ３を受理する（ステップＳ７２６）。

【０１１８】携帯電話機１００のコントローラ１１０６は、メモリカード１１０から事前に取得した再生リクエスト曲のライセンス管理ファイルからライセンスの格納されているエントリ番号を取得し（ステップＳ７２８）、その取得したエントリ番号と再生許諾要求とをメモリカードインタフェース１２００を介してメモリカード１１０へ出力する（ステップＳ７３０）。

【０１１９】メモリカード１１０のコントローラ１４２０は、エントリ番号と再生許諾要求とを受理し、エントリ番号によって指定された領域に格納されたライセンスおよび有効フラグを取得する（ステップＳ７３２）。そして、コントローラ１４２０は、有効フラグを確認する（ステップＳ７３３）。ステップＳ７３３において、有効フラグが「無」の場合、指定されたエントリにライセンスが存在しないので、再生動作が終了する（ステップＳ７４６）。ステップＳ７３３において、有効フラグが「有効」の場合、指定されたエントリにライセンスが存在するので次のステップＳ７３４へ進む。

【０１２０】そして、コントローラ１４２０は、アクセス制限情報ＡＣｍを確認する（ステップＳ７３４）。

【０１２１】ステップＳ７３４においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報ＡＣｍを確認することにより、具体的には、再生回数を確認することにより、既に再生不可の状態である場合には再生動作を終了し、アクセス制限情報の再生回数に制限がある場合にはアクセス制限情報ＡＣｍの再生回数を変更し（ステップＳ７３６）、次のステップに進む（ステップＳ７３８）。一方、アクセス制限情報ＡＣｍの再生回数によって再生が制限されていない場合においては、ステップＳ７３６はスキップされ、アクセス制限情報ＡＣｍの再生回数は変更されることなく処理が次のステップ（ステップＳ７３８）に進行される。

【０１２２】ステップＳ７３４において、当該再生動作において再生が可能であると判断された場合には、メモリ１４１５のライセンス領域１４１５Ｂに記録された再生リクエスト曲のライセンス鍵Ｋｃおよび再生制御情報ＡＣｐがバスＢＳ３上に出力される（ステップＳ７３８）。

【０１２３】得られたライセンス鍵Ｋｃと再生制御情報ＡＣｐは、切換スイッチ１４４６の接点Ｐｆを介して暗号処理部１４０６に送られる。暗号処理部１４０６は、切換スイッチ１４４２の接点Ｐｂを介して復号処理部１４１２より受けたセッションキーＫｓ３によって切換スイッチ１４４６を介して受けたライセンス鍵Ｋｃと再生制御情報ＡＣｐとを暗号化し、｛Ｋｃ／／ＡＣｐ｝Ｋｓ３をバスＢＳ３に出力する（ステップＳ７３８）。

【０１２４】バスＢＳ３に出力された暗号化データは、インタフェース１４２４、端子１４２６、およびメモリカードインタフェース１２００を介して携帯電話機１００に送出される。

【０１２５】携帯電話機１００においては、メモリカードインタフェース１２００を介してバスＢＳ２に伝達される暗号化データ｛Ｋｃ／／ＡＣｐ｝Ｋｓ３を復号処理部１５１０によって復号処理を行ない、ライセンス鍵Ｋｃおよび再生制御情報ＡＣｐを受理する（ステップＳ７４０，Ｓ７４２）。復号処理部１５１０は、ライセンス鍵Ｋｃを復号処理部１５１６に伝達し、再生制御情報ＡＣｐをバスＢＳ２に出力する。

【０１２６】コントローラ１１０６は、バスＢＳ２を介して、再生制御情報ＡＣｐを受理して再生の可否を確認する（ステップＳ７４４）。

【０１２７】ステップＳ７４４においては、再生制御情報ＡＣｐによって再生不可と判断される場合には、再生動作は終了される。

【０１２８】ステップＳ７４４において再生可能と判断された場合、コントローラ１１０６は、バスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード１１０に暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを要求する。そうすると、メモリカード１１０のコントローラ１４２０は、メモリ１４１５から暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを取得し、バスＢＳ３、インタフェース１４２４、および端子１４２６を介してメモリカードインタフェース１２００へ出力する。

【０１２９】携帯電話機１００のコントローラ１１０６は、メモリカードインタフェース１２００およびバスＢＳ２を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを取得し、バスＢＳ２を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃをコンテンツ再生デバイス１５５０へ与える。

【０１３０】そして、コンテンツ再生デバイス１５５０の復号処理部１５１６は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを復号処理部１５１０から出力されたライセンス鍵Ｋｃによって復号してコンテンツデータＤｃを取得する。

【０１３１】そして、復号されたコンテンツデータＤｃは音楽再生部１５１８へ出力され、音楽再生部１５１８は、コンテンツデータ｛Ｄｃ｝Ｋｃを再生し、ＤＡ変換器１５１９はディジタル信号をアナログ信号に変換して端子１５３０へ出力する。そして、音楽データは端子１５３０から外部出力装置を介してヘッドホーン１３０へ出力されて再生される。これによって再生動作が終了する（ステップＳ７４６）。

【０１３２】メモリカード１１１，１１２に記録された暗号化コンテンツデータのそれぞれ携帯電話機１０１，１０２における再生動作も図１１に示すフローチャートに従って行なわれる。

【０１３３】携帯電話機１００～１０２は、それぞれ、メモリカード１１０～１１２が装着されると、メモリカ

ード１１０～１１２に記録された暗号化コンテンツデータを管理するためのデータベースを作成し、その作成したデータベースをＲＡＭ１１０３に格納する。図１２を参照して、携帯電話機１００～１０２におけるデータベースの作成について説明する。

【０１３４】図１２を参照して、データベース１５０は、コンテンツＮｏ１５３１、コンテンツＩＤ１５３２、タイトル名１５３３、アーティスト名１５３４、コンテンツ種別１５３５、ライセンス有無１５３６、および格納カードＩＤ１５３７を含む。携帯電話機１００のコントローラ１１０６は、メモリカード１１０が装着されると、バスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード１１０のメモリ１４１５のデータ領域１４１５Ｃから付加情報Ｄｃ－ｉｎｆ、エントリ番号およびカードＩＤを読出す。そして、読出した付加情報Ｄｃ－ｉｎｆに含まれるコンテンツＩＤ、タイトル名、アーティスト名、およびコンテンツ種別を、それぞれ、データベース１５０のコンテンツＮｏ１５３１、コンテンツＩＤ１５３２、タイトル名１５３３、アーティスト名１５３４、およびコンテンツ種別１５３５に格納する。また、コントローラ１１０６は、読出したエントリ番号に基づいて対応するコンテンツデータのライセンスの有無をライセンス有無１５３６に格納する。すなわち、コントローラ１１０６は、メモリカード１１０からエントリ番号を読出すことができれば、ライセンスが有ると認識し、エントリ番号を読出すことができなければ、ライセンスが無いと認識する。また、コントローラ１１０６は、メモリカード１１０から読出したカードＩＤを格納カードＩＤ１５３７に格納する。

【０１３５】コントローラ１１０６は、携帯電話機１００に複数のメモリカードが、順次、装着された場合、その全てのメモリカードに格納されている暗号化コンテンツデータについてのデータベースを作成する。したがって。図１２においては、格納カードＩＤ１５３７には、複数のカードＩＤが示されており、コンテンツＮｏ１５３１が１～Ｎのコンテンツは、相互に異なるメモリカードに格納されていることを表している。そして、コントローラ１１０６は、作成したデータベース１５０をＲＡＭ１１０３に格納する。

【０１３６】携帯電話機１０１，１０２も、携帯電話機１００の場合と同様にして装着されたメモリカードに格納された暗号化コンテンツデータを管理するためのデータベースを作成し、その作成したデータベースをＲＡＭ１１０３に格納する。

【０１３７】図１３および図１４を参照して、携帯電話機１００が配信サーバ１０から受信した暗号化コンテンツデータおよびライセンスをメモリカード１１０に記録し、メモリカード１１０に記録した暗号化コンテンツデータを管理するためのデータベースを作成した段階で携帯電話機１００のユーザが可能な動作について説明する。この段階で、携帯電話機１００の表示パネル１１１０には、図１３に示す画面１７０が表示されている。

【０１３８】携帯電話機１００のユーザは、友人である携帯電話機１０１，１０２のユーザから携帯電話機１０１，１０２のＲＡＭ１１０３に格納されたデータベースを送信して貰うことが可能である。

【０１３９】図１３を参照して、携帯電話機１００のユーザは、表示パネル１１１０の画面１７０を見て、「所有曲情報の取得」を選択し、「決定」を押すと表示パネル１１１０には、画面１７１が表示される。画面１７１は、携帯電話機１０１，１０２からデータベースを送信して貰うときの通信方法を携帯電話機１００のユーザに問う画面である。携帯電話機１００のユーザは、たとえば、「ケーブル接続」を選択して「決定」を押す。そうすると、表示パネル１１１０には、「ケーブルを接続して「開始」を押してください」とのコメントの画面１７２が表示される。携帯電話機１００のユーザは、自己の携帯電話機１００をケーブルによって携帯電話機１０１，１０２と接続して「開始」を押す。

【０１４０】そして、表示パネル１１１０には、「取得中・・・」のメッセージを示す画面１７３が表示される。所有曲情報の取得が終了すると、表示パネル１１１０には、取得が完了した旨のメッセージを示す画面１７４が表示される。このようにして、携帯電話機１００のユーザは、携帯電話機１０１，１０２からデータベースを受信する。そして、携帯電話機１００のコントローラ１１０６は、受信したベータベースをＲＡＭ１１０３に格納する。したがって、ＲＡＭ１１０３には、図１２に示すようなデータベースが複数個格納される。携帯電話機１００のコントローラ１１０６は、ＲＡＭ１１０３に複数のデータベースが格納されると、図１５に示すような複数のデータベースを管理するための一覧表１５５を作成し、ＲＡＭ１１０３に格納する。

【０１４１】一覧表１５５は、データベースＮｏ１５５１、コンテンツデータベース１５５２、コンテンツ数１５５３、端末ＩＤ１５５４、および所有者名１５５５を含む。データベースＮｏ１５５１は、各データベースに付与される整理番号である。なお、「１」は、自己の携帯電話機に保持されたデータベースであることを示す。コンテンツデータベース１５５２は、複数のデータベースを識別ための情報である。コンテンツ数１５５３は、各データベースに含まれるコンテンツ数を示す。端末ＩＤ１５５４は、各データベースを保持する携帯電話機を特定する情報である。端末ＩＤとしては、たとえば、携帯電話機の電話番号が考えられる。所有者名１５５５は、各データベースの所有者を表す。

【０１４２】このように、携帯電話機１００のコントローラ１１０６は、携帯電話機１０１，１０２からデータベースを受信すると、一覧表１５５を作成し、その作成した一覧表１５５をＲＡＭ１１０３に格納する。

【０１４３】再び、図１３を参照して、携帯電話機１００のユーザが画面１７０において、「曲の購入」を選択して「決定」を押すと、画面１７５が表示パネル１１１０に表示される。つまり、新たに購入したい曲の検索方法を携帯電話機１００のユーザに問う画面が表示される。携帯電話機１００のユーザは、「アーティスト名」を選択して「決定」を押すと、検索したいアーティスト名の入力を促す画面１７６が表示パネル１１１０に表示される。

【０１４４】携帯電話機１００のユーザは、「アーティストＡ」を入力して「検索開始」を押す。入力された「アーティストＡ」は携帯電話機１００から配信サーバ１０へ送信される。そして、配信サーバ１０は、携帯電話機１００から受信した「アーティストＡ」によってアーティストＡが作曲した音楽データのコンテンツＩＤとタイトル名とを検索し、その検索結果を携帯電話機１００へ送信する。

【０１４５】そうすると、携帯電話機１００においては、検索結果を配信サーバ１０から受信し、アーティストＡが作曲した曲のタイトル名、その曲を所有している者、その曲のライセンスがその曲を格納している場所に存在するか否かを示す情報が画面１７７として表示パネル１１１０に表示される。

【０１４６】画面１７７が表示パネル１１１０に表示された時点で、携帯電話機１００のユーザが「タイトル４」の曲を選択すると、表示パネル１１１０に画面１７８が表示される。「タイトル４」の曲は、Ｂさんが所有しており、ライセンスが無いので、Ｂさんの携帯電話機を介してＢさんのメモリカードに格納された暗号化コンテンツデータをコピー（複製）することになる。そこで、次に、表示パネル１１１０にＢさんの携帯電話機から暗号化コンテンツデータをコピーするときの通信方法を問合わせる画面１７８が表示される。携帯電話機１００のユーザは、画面１７８において、「ケーブル接続」を選択して「決定」を押すと、「ケーブルを接続して準備ができたら「開始」を押してください。」とのメッセージが表示される（画面１７９）。携帯電話機１００のユーザは、自己の携帯電話機１００をケーブルによってＢさんの携帯電話機と接続し、「開始」を押す。

【０１４７】図１４を参照して、表示パネル１１１０には、「コピー許可の問合わせ中」のメッセージが表示される（画面１８０）。Ｂさんがタイトル４のコンテンツが格納されているメモリカードを装着してコピーを許可すると、「コピーが許可され、タイトル４のコンテンツをコピーしています」というメッセージとコピーの進行状況とが表示パネル１１１０に表示される（画面１８１）。Ｂさんのメモリカードから暗号化コンテンツデータのコピーが終了すると、「「タイトル４」の取得に成功した」ことを示すメッセージが表示されるとともに、「ライセンスを取得する場合には、「ライセンスの取得」を押してください」とのメッセージが表示される（画面１８２）。そして、携帯電話機１００のユーザが「ライセンスの取得」を押すと、画面１８３に移行する。

【０１４８】図１３に示す画面１７７において、「タイトル３」を選択した場合、「タイトル３」のコンテンツは、携帯電話機１００のユーザに保持され、ライセンスが無いので、図１４に示す画面１８３に移行する。

【０１４９】画面１８３においては、「配信サーバ１０に接続して「タイトルｎ」のライセンスを取得しています」というメッセージが表示パネル１１１０に表示される（画面１８３）。そして、ライセンスの取得が終了すると、「「タイトルｎ」のライセンスの取得が完了いたしました」というメッセージが表示パネル１１１０に表示される（画面１８４）。なお、図１３に示す画面１７７において、携帯電話機１００のユーザが「タイトル２」を選択した場合、「タイトル２」のコンテンツおよびライセンスは、携帯電話機１００のユーザに保持されているので、暗号化コンテンツデータのコピーまたはライセンスの配信サーバ１０からの受信は行なわれない。また、画面１７７において、携帯電話機１００～１０２に装着されるメモリカード１１０～１１２に配信されていない暗号化コンテンツデータが選択された場合、図７および図８に示すフローチャートに従って暗号化コンテンツデータおよびライセンスの配信動作が実行される。

【０１５０】携帯電話機１００は、他の携帯電話機から暗号化コンテンツデータをコピーし、そのコピーした暗号化コンテンツデータのライセンスを配信サーバ１０から受信したとき、暗号化コンテンツデータおよびライセンスをメモリカード１１０に記録するとともに、メモリカード１１０に格納されている暗号化コンテンツデータを管理するためのデータベースを更新する。

【０１５１】図１６および図１７を参照して、図１３に示す画面１７５～１７７における動作を詳細に説明する。図１６は、配信サーバ１０における暗号化コンテンツデータの検索動作を説明するためのフローチャートである。また、図１７は、配信サーバ１０における検索結果を受信した携帯電話機１００が、検索結果に記載された暗号化コンテンツデータを自己が保持するデータベースに基づいて検索する動作を説明するためのフローチャートである。

【０１５２】図１６を参照して、検索動作が開始されると、携帯電話機１００のユーザは、アーティストＡをキー操作部１１０８から入力してコンテンツの検索を配信サーバ１０へ問い合わせる（ステップＳ２００）。配信サーバ１０は、携帯電話機１００からアーティストＡを受信し、配信制御部３１５は、バスＢＳ１を介して情報データベース３０４に格納された暗号化コンテンツデータの付加情報Ｄｃ－ｉｎｆに基づいてアーティストＡのコンテンツを検索し、その検索結果をバスＢＳ１および

通信装置３５０を介して携帯電話機１００へ送信する。この場合、配信サーバ１０は、図１８に示すようなコンテンツ数Ｓ、コンテンツＩＤ、およびタイトル名の一覧表を検索結果として携帯電話機１００へ送信する。

【０１５３】そうすると、携帯電話機１００のコントローラ１１０６は、アンテナ１１０１および送受信部１１０２を介して検索結果を受信し、配信サーバ１０で検出されたコンテンツ数Ｓを取得して検索結果のコンテンツ数をＳに設定する（ステップＳ２０２）。そして、コントローラ１１０６は、検索結果データベースを作成する（ステップＳ２０４）。つまり、コントローラ１１０６は、図１９に示すように配信サーバ１０において検索されたコンテンツ数をＳに設定した検索結果データベースを作成する。

【０１５４】その後、コントローラ１１０６は、配信サーバ１０から受信した検索結果（図１８参照）のコンテンツＩＤおよびタイトル名を取得し、図１９に示す検索結果データベースのコンテンツＩＤの欄およびタイトル名の欄に、それぞれ、取得したコンテンツＩＤおよびタイトル名を格納する（ステップＳ２０６）。そして、コントローラ１１０６は、検索結果データベース（図１９参照）の所有端末数の欄および所有端末ＩＤの欄を全て「０」に初期化する（ステップＳ２０８）。コントローラ１１０６は、さらに、検索結果データベースのライセンス有無の欄を全て「０」に初期化して（ステップＳ２１０）、コンテンツの検索動作が終了する。

【０１５５】その後、図１７に示すフローチャートが実行される。携帯電話機１００が配信サーバ１０から受信した検索結果（図１８参照）に含まれるコンテンツＩＤ（１）～コンテンツＩＤ（Ｓ）によって特定されるコンテンツを、携帯電話機１００のＲＡＭ１１０３に格納されたデータベースを参照して検索する動作が開始されると、ｍ＝１に設定され（ステップＳ３００）、ｎ＝１に設定され（ステップＳ３０２）、ｓ＝１に設定される（ステップＳ３０４）。ここで、ｍは、ＲＡＭ１１０３に格納されたデータベースの数を表し、ｎは、各データベースに含まれるコンテンツ数を表し、ｓは、検索結果データベース（図１９参照）に含まれるコンテンツ数を表す。

【０１５６】ステップＳ３０４の後、携帯電話機１００のコントローラ１１０６は、検索結果データベースのコンテンツＩＤ（１）がＲＡＭ１１０３に格納されたデータベース（１）に含まれるコンテンツＩＤに一致するか否かを判定する（ステップＳ３０６）。ステップＳ３０６において、検索結果データベースのコンテンツＩＤ（１）がデータベース（１）に含まれるコンテンツＩＤに一致すると判定されたとき、コントローラ１１０６は、データベース（１）を保持する端末ＩＤをＲＡＭ１１０３に格納された一覧表１５５（図１５参照）から読出し、その読出した端末ＩＤを検索結果データベースの所有端末ＩＤの欄に格納する（ステップＳ３０８）。また、コントローラ１１０６は、データベース（１）（図１２参照）からコンテンツＩＤ（１）に対応するライセンス有無を読出し、その読出したライセンス有無を検索結果データベースのライセンス有無の欄に格納する（ステップＳ３１０）。その後、ステップＳ３１２へ移行する。

【０１５７】また、ステップＳ３０６において、検索結果データベースのコンテンツＩＤ（１）がデータベース（１）に含まれるコンテンツＩＤに一致しないと判定されたときもステップＳ３１２へ移行する。ステップＳ３１２において、ｓ＝ｓ＋１に設定され（ステップＳ３１２）、コントローラ１１０６は、ｓ＝Ｓか否かを判定する（ステップＳ３１４）。ここで、Ｓは、配信サーバ１０において検索されたコンテンツの総数である（図１９参照）。ステップＳ３１４においてｓ＝Ｓであると判定されたとき、ステップＳ３１６へ移行する。また、ステップＳ３１４においてｓ＝Ｓでないと判定されたとき、ステップＳ３０６～Ｓ３１４が繰返される。すなわち、ステップＳ３０６～Ｓ３１４は、検索結果データベースに含まれるコンテンツＩＤ（１）～コンテンツＩＤ（Ｓ）がデータベース（１）に含まれるコンテンツＩＤ（１）に一致するか否かを判定し、一致すれば、その一致したコンテンツＩＤ（１）に対応するライセンスの有無とコンテンツＩＤ（１）を含むデータベースを保持する端末ＩＤとをＲＡＭ１１０３に格納されたデータベース（図１２参照）および一覧表（図１５参照）から読出し、検索結果データベースに格納するステップである。

【０１５８】ステップＳ３１４において、ｓ＝Ｓであると判定されたとき、ｎ＝ｎ＋１に設定され、コントローラ１１０６は、ｎ＝Ｎ（ｍ）であるか否かを判定する（ステップＳ３１８）。ステップＳ３１８においてｎ＝Ｎ（ｍ）でないと判定されたとき、ステップＳ３０４～Ｓ３１８が繰返される。この場合は、ＲＡＭ１１０３に格納されたデータベース（１）の全てのコンテンツＩＤ（１）～コンテンツＩＤ（Ｎ（ｍ））と検索結果データベースのコンテンツＩＤ（１）～コンテンツＩＤ（Ｓ）とが一致するか否かの判定が行なわれる。

【０１５９】そして、ステップＳ３１８においてｎ＝Ｎ（ｍ）であると判定されたとき、ｍ＝ｍ＋１に設定され（ステップＳ３２０）、コントローラ１１０６は、ｍ＝Ｍであるか否かを判定する（ステップＳ３２２）。ここで、Ｍは、ＲＡＭ１１０３に格納されたデータベースの総数を表す。ステップＳ３２２においてｍ＝Ｍでないと判定されたとき、ステップＳ３０２～Ｓ３２２が繰返される。すなわち、ＲＡＭ１１０３に格納されたＭ個のデータベースに検索結果データベースのコンテンツＩＤ（１）～コンテンツＩＤ（Ｓ）が含まれるか否かが判定される。そして、ステップＳ３２２において、ｍ＝Ｍであると判定されたとき、データベースの検索動作が終了

する（ステップＳ３２４）。その結果、図１９に示す検索結果データベースの所有端末ＩＤ１，２，・・・の欄、およびライセンス有無の欄にデータが格納される。そして、コントローラ１１０６は、各コンテンツＩＤを含むデータベースを保持する端末ＩＤの個数を所有端末数の欄に格納する。図１９においては、コンテンツＩＤ（６）に対応する所有端末数が「２」になっているが、これは、コンテンツＩＤ（６）を含むデータベースが２つの端末に保持されていることを示す。なお、所有端末ＩＤ１，２，・・・は、コンテンツＩＤ（１）～コンテンツＩＤ（Ｓ）を含むデータベースが保持されている端末が判明した順序を示す。したがって、１番目に判定した端末ＩＤは所有端末ＩＤ１の欄に格納される。以下、同様にして２番目、３番目、・・・に判定した端末ＩＤが所有端末ＩＤ２，ＩＤ３，・・・の欄に格納される。

【０１６０】このように、携帯電話機１００のコントローラ１１０６は、配信サーバ１０から検索結果を受信したとき、検索結果データベースを作成する。そして、コントローラ１１０６は、作成した検索結果データベースからタイトル名、所有端末ＩＤ、およびライセンス有無を抽出し、タイトル名、所有端末ＩＤから判明する所有者、およびライセンスの有無を表示パネル１１１０に画面１７７（図１３参照）として表示する。

【０１６１】また、図１３の画面１７８，１７９および図１４の画面１８０～１８２によって表される携帯電話機１０１，１０２からの暗号化コンテンツデータのコピー（複製）は、図２０に示すフローチャートに従って行なわれる。携帯電話機１０１，１０２に装着されたメモリカード１１１，１１２から携帯電話機１００に装着されたメモリカード１１０へ暗号化コンテンツデータをコピーする場合、携帯電話機１０１，１０２のコントローラ１１０６と携帯電話機１００のコントローラ１１０６とがデータの授受に関与するが、図２０においては、説明の便宜上、１つのコントローラを示し、その１つのコントローラは、携帯電話機１０１，１０２のコントローラ１１０６の機能と携帯電話機１００のコントローラ１１０６の機能とを果たすこととしている。また、図２０に示す処理に入る前に、送信側である携帯電話機１０１，１０２のユーザは、メモリカード１１１，１１２を携帯電話機１０１，１０２に装着し、携帯電話機１００のユーザからの暗号化コンテンツデータのコピー要求に対して許可を与えているものとする。

【０１６２】図２０を参照して、複製リクエストがユーザから指示されると（ステップＳ４００）、携帯電話機１００のコントローラ１１０６は、メモリカード１１０へ認証データの送信要求をメモリカードインタフェース１２００を介してメモリカード１１０へ送信する（ステップＳ４０２）。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ３を介して認証データの送信要求を受信する（ステップＳ４０４）。

【０１６３】メモリカード１１０のコントローラ１４２０は、認証データの送信要求を受信すると、認証データ保持部１４００から認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ３を介して読出し、その読出した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ３、インタフェース１４２４および端子１４２６を介してメモリカードインタフェース１２００へ出力する（ステップＳ４０６）。そして、携帯電話機１００のコントローラ１１０６は、メモリカードインタフェース１２００を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを受取り、送受信部１１０２およびアンテナ１１０１を介して携帯電話機１０１，１０２へメモリカード１１０の認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを送信する（ステップＳ４０８）。

【０１６４】そうすると、携帯電話機１０１，１０２のコントローラ１１０６は、アンテナ１１０１および送受信部１１０２を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを受信し、バスＢＳ２およびメモリカードインタフェース１２００を介してメモリカード１１１，１１２へ認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを入力する（ステップＳ４０８）。メモリカード１１１，１１２のコントローラ１４２０は、端子１４２６およびインタフェース１４２４を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを受信し、その受信した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ３を介して復号処理部１４０８へ与える。そして、復号処理部１４０８は、ＫＰａ保持部１４１４からの認証鍵ＫＰａによって認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａの復号処理を実行する（ステップＳ４１０）。コントローラ１４２０は、復号処理部１４０８における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード１１０が正規のメモリカードであって、メモリカード１１０から正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ４１２）。正当な認証データであると判断された場合、コントローラ１４２０は、認証データから取得されたクラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を承認し、受理する。そして、次の処理（ステップＳ４１４）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を受理しないで処理を終了する（ステップＳ４２０）。

【０１６５】認証の結果、正当な認証データを持つメモリカードへの暗号化コンテンツデータの複製であることが確認されると、メモリカード１１１，１１２において、コントローラ１４２０は、バスＢＳ３を介してメモリ１４１５のデータ領域１４１５Ｃから暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを読出し、バスＢＳ３、インタフェース１４２４および端子

１４２６を介して｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆを出力する（ステップＳ４１４）。携帯電話機１０１，１０２のコントローラ１１０６は、メモリカードインタフェース１２００およびバスＢＳ２を介して｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆを受理し、送受信部１１０２およびアンテナ１１０１を介して｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆを携帯電話機１００へ送信する（ステップＳ４１６）。

【０１６６】携帯電話機１００のコントローラ１１０６は、アンテナ１１０１および送受信部１１０２を介して｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆを受信し、バスＢＳ２およびメモリカードインタフェース１２００を介して｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆをメモリカード１１０へ入力し、メモリカード１１０のコントローラ１４２０は、端子１４２６およびインタフェース１４２４を介して｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆを受取る。そして、コントローラ１４２０は、バスＢＳ３を介して｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆをメモリ１４１５のデータ領域１４１５Ｃに格納して（ステップＳ４１８）、暗号化コンテンツデータの複製動作が終了する（ステップＳ４２０）。

【０１６７】携帯電話機１００のユーザは、暗号化コンテンツデータの複製が終了した後、図７および図８に示したフローチャートに従って、複製した暗号化コンテンツデータを復号および再生するためのライセンスの配信要求を配信サーバ１０へ送信し、配信サーバ１０からライセンスを受信してメモリカード１１０に格納する。

【０１６８】このように、携帯電話機１００のユーザは、新たに購入したい曲が携帯電話機１０１，１０２に装着されるメモリカード１１１，１１２に格納されていることを確認すると、携帯電話機１０１，１０２から暗号化コンテンツデータを複製し、その複製した暗号化コンテンツデータのライセンスを配信サーバ１０から受信する。

【０１６９】この発明の実施の形態によれば、携帯電話機のユーザは、新たに購入したい曲がどこに格納されているかを検索した後、暗号化コンテンツデータが格納されているメモリカードから暗号化コンテンツデータを複製するので、購入したい曲の受信に長時間を必要とせず、そのための通信費を節約できる。

【０１７０】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【０１７１】

【発明の効果】本発明によれば、携帯電話機のユーザは、新たに購入したい曲がどこに格納されているかを検索した後、暗号化コンテンツデータが格納されているメモリカードから暗号化コンテンツデータを複製するので、購入したい曲の受信に長時間を必要とせず、そのための通信費を節約できる。

【図面の簡単な説明】

【図１】　データ配信システムを概念的に説明する概略図である。

【図２】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図３】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図４】　図１に示すデータ配信システムにおける配信サーバの構成を示す概略ブロック図である。

【図５】　図１に示すデータ配信システムにおける携帯電話機の構成を示す概略ブロック図である。

【図６】　図１に示すデータ配信システムにおけるメモリカードの構成を示す概略ブロック図である。

【図７】　図１に示すデータ配信システムにおける配信動作を説明するための第１のフローチャートである。

【図８】　図１に示すデータ配信システムにおける配信動作を説明するための第２のフローチャートである。

【図９】　メモリカードにおける再生リストファイルの構成を示す図である。

【図１０】　図９に示すコンテンツファイルに記録された暗号化コンテンツデータと付加情報との関係を示す概念図である。

【図１１】　携帯電話機における再生動作を説明するためのフローチャートである。

【図１２】　暗号化コンテンツデータを管理するためのデータベースの概念図である。

【図１３】　携帯電話機における各動作時に表示パネルに示される画面を示す図である。

【図１４】　携帯電話機における各動作時に表示パネルに示される画面を示す図である。

【図１５】　複数のデータベースを管理するための一覧表の概念図である。

【図１６】　購入したい曲の配信サーバにおける検索動作を説明するためのフローチャートである。

【図１７】　配信サーバから受信した検索結果に含まれる暗号化コンテンツデータの携帯電話機における検索動作を説明するためのフローチャートである。

【図１８】　配信サーバから送信される検索結果の例である。

【図１９】　携帯電話機における検索結果を示すデータベースの概念図である。

【図２０】　他の携帯電話機からの暗号化コンテンツデータの複製動作を説明するためのフローチャートである。

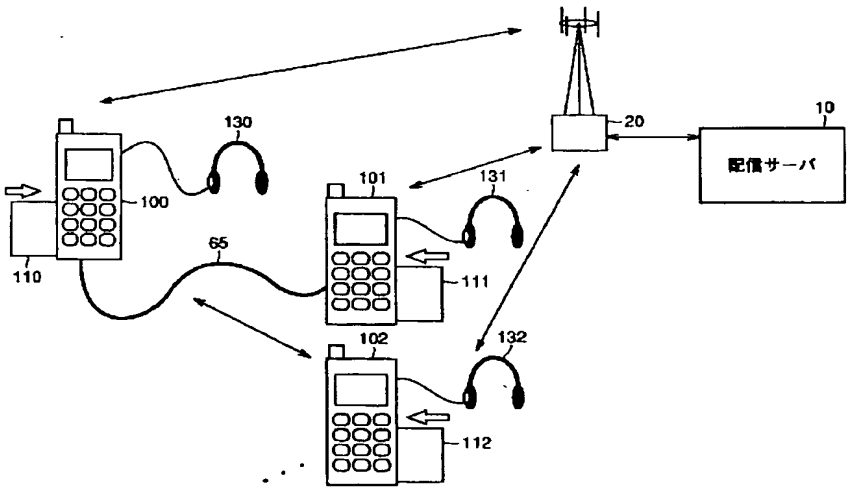
【符号の説明】

１０　配信サーバ、２０　配信キャリア、６５　専用ケーブル、１００～１０２　携帯電話機、１１０～１１２　メモリカード、１３０～１３２　ヘッドホーン、１５０　データベース、１５５　一覧表、１６０　再生リス

トファイル、１６３　コンテンツ管理情報、１６５　エントリ管理情報、１６６　カードＩＤ、１７０～１８４　画面、３０２　課金データベース、３０４　情報データベース、３０７　メニューデータベース、３０８　配信記録データベース、３１０　データ処理部、３１２，３２０，１４０４，１４０８，１４１２，１４２２，１５０４，１５１０，１５１６　復号処理部、３１３　認証鍵保持部、３１５　配信制御部、３１６，１４１８，１５０８　セッションキー発生部、３１８，３２６，３２８，１４０６，１４１０，１４１７，１５０６　暗号処理部、３５０　通信装置、１１０１　アンテナ、１１０２　送受信部、１１０３　ＲＡＭ、１１０６，１４２０　コントローラ、１１１２　ＵＳＢインタフェース、１１１４，１４２６，１５３０　端子、１１０８　キー操作部、１１１０　表示パネル、１２００　メモリカードインタフェース、１４００，１５００　認証データ保＊

＊持部、１４０２　Ｋｍｃ保持部、１４１４　ＫＰａ保持部、１４１５　メモリ、１４１５Ａ　ログ領域、１４１５Ｂ　ライセンス領域、１４１５Ｃ　データ領域、１４１６　ＫＰｍｃ保持部、１４２１　Ｋｍ保持部、１４２４　インタフェース、１４４２，１４４６　切換スイッチ、１５０２　Ｋｐｌ保持部、１５１８　音楽再生部、１５１９　ＤＡ変換器、１５３１　コンテンツＮｏ、１５３２　コンテンツＩＤ、１５３３　タイトル名、１５３４　アーティスト名、１５３５　コンテンツ種別、１５３６　ライセンス有無、１５３７　格納カードＩＤ、１５５０コンテンツ再生デバイス、１５５１　データベースＮｏ、１５５２　データベース、１５５３　コンテンツ数、１５５４　端末ＩＤ、１５５５　所有者名、１６２１～１６２ｎ　ライセンス管理ファイル、１６１１～１６１ｎ　コンテンツファイル、１６３１～１６４０　コンテンツデータ、１６５１～１６６０　管理情報。

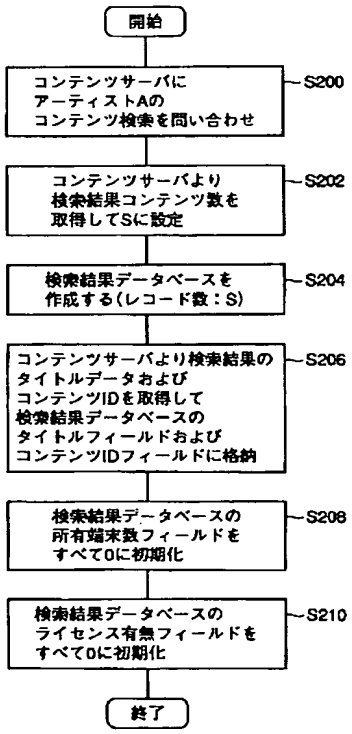
【図１】



【図２】

記号	種類	属性	特性
Dc	コンテンツデータ	コンテンツ固有	例：音楽データ、朗読データ、教材データ、画像データ Kcにて復号可能な暗号化コンテンツデータ {Dc}Kcとして配信され、メモリカードに保持される
Dc-inf	付加情報	コンテンツ固有	Dcに付随する平文データ。
Kc	ライセンス	コンテンツ固有	ライセンス 暗号化コンテンツデータを復号する復号鍵
ACm/ACp	ライセンス	ライセンス固有	制限情報 再生やライセンスの取り扱いに対する制限事項
コンテンツID	ライセンス	コンテンツ固有	コンテンツを特定するための管理コード
ライセンスID	ライセンス	ライセンス固有	ライセンスを特定するための管理コード
ライセンス	ライセンス	ライセンス固有	Kc+ACm+ACp+コンテンツID+ライセンスIDの総称
有効フラグ	フラグ	ライセンス固有	ライセンスをメモリカードから外部へ出すことが可能か否かを表す。

【図１６】



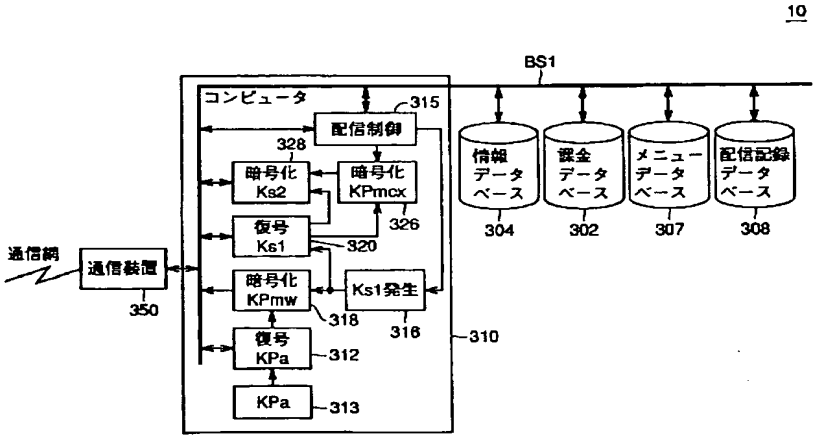
【図１８】

No	コンテンツID	タイトル名
1	878172	タイトル1
2	231243	タイトル2
3	434345	タイトル3
4	344567	タイトル4
5	324325	タイトル5
6	434255	タイトル6
⋮	⋮	⋮
S	322432	タイトルS

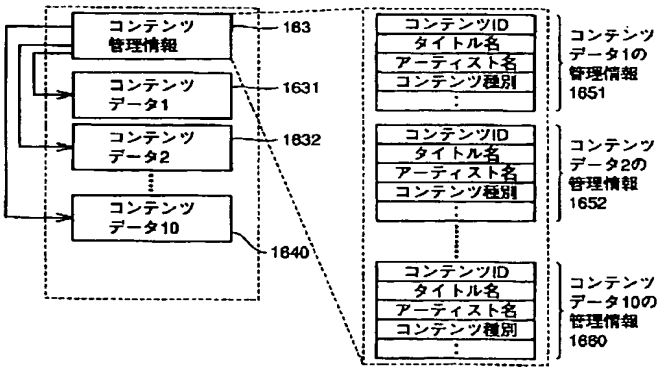
【図３】

	記号	種類	属性	特性
配信サーバ	KPa	公開認証鍵	システム共通	認証局にて認証データを復号する鍵
	Ks1	共通鍵	セッション固有	メモリカードへのライセンス配信ごとに発生
メモリカード	KPa	公開認証鍵	システム共通	認証局にて認証データを復号する鍵 配信サーバのKPaと同一
	KPmw	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 wはクラスを識別するための識別子
	Kmw	秘密復号鍵	クラス固有	公開暗号鍵KPmwにて暗号化されたデータを復号する非対称な復号鍵
	KPmcx	公開暗号鍵	個別	メモリカードごとに異なる。 xはモジュールを識別するための識別子
	Kmcx	秘密復号鍵	個別	公開暗号鍵KPmcxにて暗号化されたデータを復号する非対称な復号鍵
	Ks2	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール間のライセンスの授受ごとに発生
	Cmw	証明書	クラス証明書	メモリカードのクラス証明書。 認証機能を有する。 (KPmw//Cmw)KPaの形式で出荷時に記録。 ＊メモリカードのクラスwごとに異なる。
コンテンツ再生デバイス	KPpy	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 yはクラスを識別するための識別子
	Kpy	秘密復号鍵	クラス固有	公開暗号鍵KPpyにて暗号化されたデータを復号する非対称な復号鍵
	Ks3	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール間の再生セッションごとに発生
	Cpy	証明書	クラス証明書	コンテンツ再生デバイスのクラス証明書。認証機能を有する。 (KPpy//Cpy)KPaの形式で出荷時に記録。 ＊コンテンツ再生デバイスのクラスyごとに異なる。

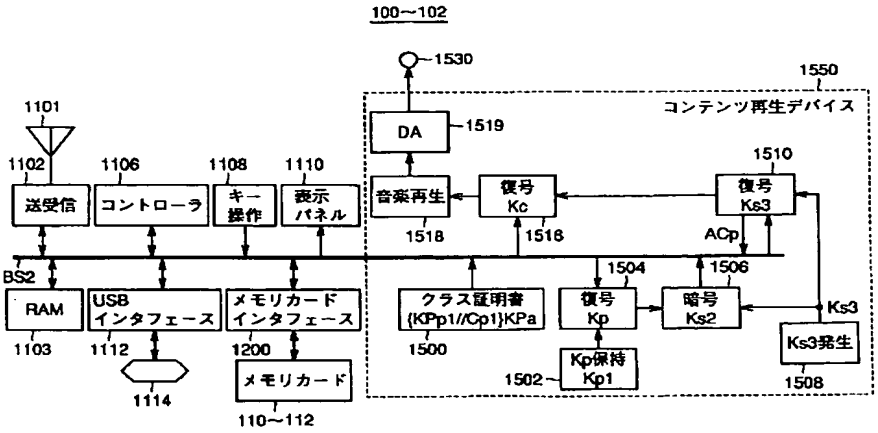
【図４】



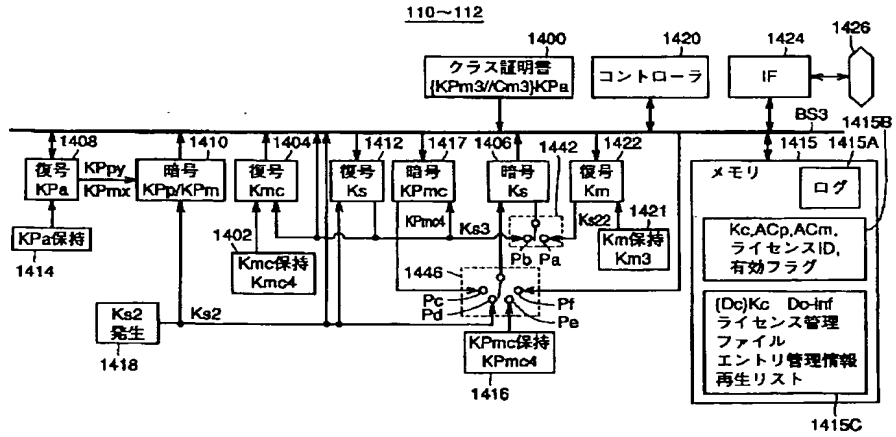
【図１０】



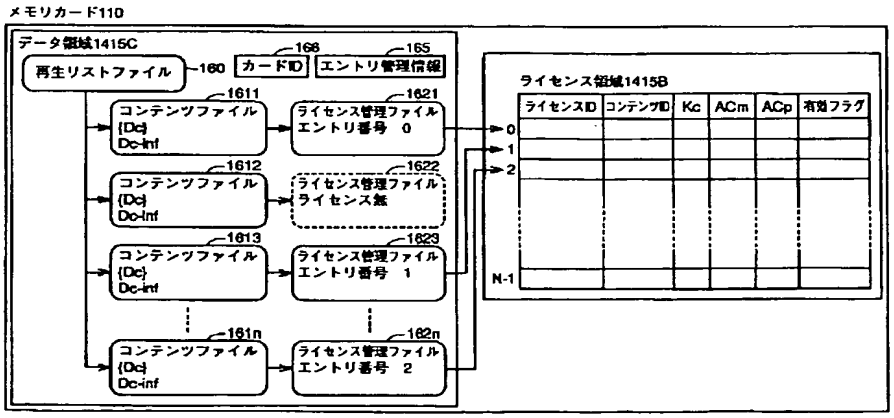
【図５】


100～102
1530
1550
コンテンツ再生デバイス
1101
DA
1519
1102
1106
1108
1110
送受信
コントローラ
キー操作
表示パネル
音楽再生
復号 Kc
1518
1518
1510
復号 Ks3
ACp
BS2
1504
1506
RAM
USB インタフェース
メモリカード インタフェース
クラス証明書 {KPp1//Cp1}KPa
復号 Kp
暗号 Ks2
Ks3
Ks3発生
1103
1112
1200
1500
Kp保持 Kp1
1502
1508
1114
メモリカード
110～112

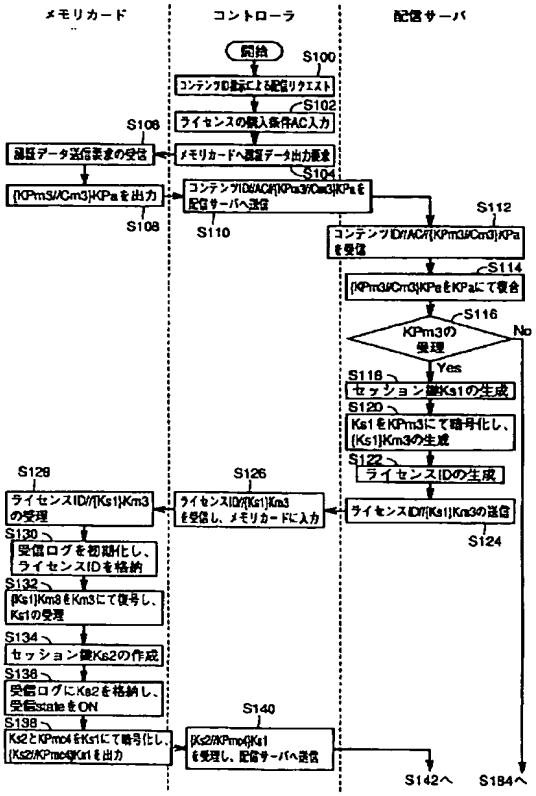
【図６】


110～112
1400
1420
1424
1426
クラス証明書 {KPm3//Cm3}KPa
コントローラ
IF
BS3
1415B
1408
1410
1404
1412
1417
1406
1442
1422
1415
1415A
復号 KPa
KPpy KPmx
暗号 KPp/KPm
復号 Kmc
復号 Ks
暗号 KPmc
暗号 Ks
復号 Km
メモリ
ログ
KPmc4
Ks3
Ks22
1421
Pb Pa
Km保持 Km3
KPa保持
1414
1402
Kmc保持 Kmc4
Kc,ACp,ACm, ライセンスID, 有効フラグ
1446
Pc
Pd
Pf
Pe
Ks2
Ks2 発生
1418
KPmc保持 KPmc4
1416
{Dc}Kc Do-Inf ライセンス管理 ファイル エントリ管理情報 再生リスト
1415C

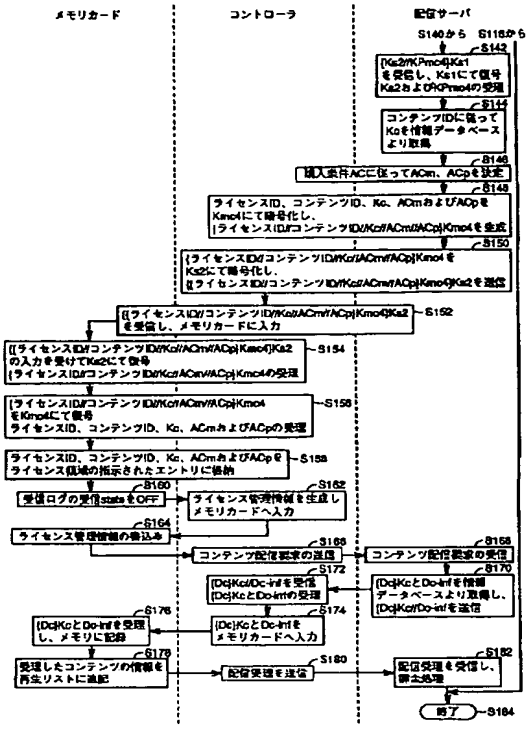
【図９】


メモリカード110
データ領域1415C
再生リストファイル
160
カードID
168
エントリ管理情報
165
コンテンツファイル {Dc} Dc-Inf
1611
ライセンス管理ファイル エントリ番号 0
1621
コンテンツファイル {Dc} Dc-Inf
1612
ライセンス管理ファイル ライセンス無
1622
コンテンツファイル {Dc} Dc-Inf
1613
ライセンス管理ファイル エントリ番号 1
1623
コンテンツファイル {Dc} Dc-Inf
161n
ライセンス管理ファイル エントリ番号 2
162n
ライセンス領域1415B
ライセンスID
コンテンツID
Kc
ACm
ACp
有効フラグ
0
1
2
N-1

【図７】



【図８】



【図１２】

150

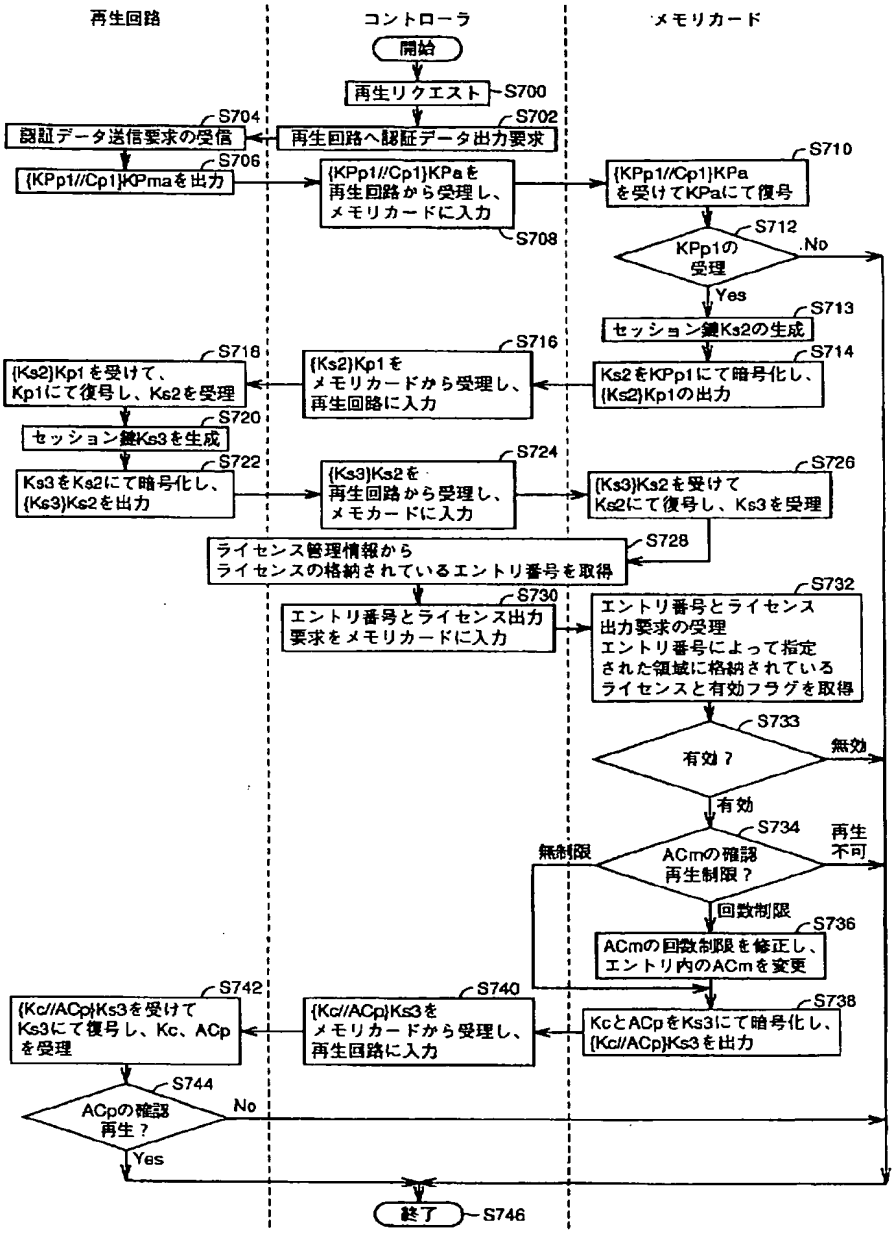
1531 コンテンツNo	1532 コンテンツID	1533 タイトル名	1534 アーティスト名	1535 コンテンツ種別	-------	1536 ライセンス有無	1537 格納カードID
1	CONTID(1)	タイトル1	アーティスト1	ロック		1	CARDID(1)
2	CONTID(2)	タイトル2	アーティスト2	クラシック		1	CARDID(2)
3	CONTID(3)	タイトル3	アーティスト3	英会話		0	CARDID(3)
：	：	：	：	：		：	：
N	CONTID(N)	タイトルN	アーティストN	ニュース		1	CARDID(4)

【図１５】

155

1551 データベースNo	1552 コンテンツデータベース	1553 コンテンツ数	1554 端末ID	1555 所有者名
1	コンテンツデータベース(1)	N(1)	端末ID(1)	OWNER(1)
2	コンテンツデータベース(2)	N(2)	端末ID(2)	OWNER(2)
3	コンテンツデータベース(3)	N(3)	端末ID(3)	OWNER(3)
：	：	：	：	：
M	コンテンツデータベース(M)	N(M)	端末ID(M)	OWNER(M)

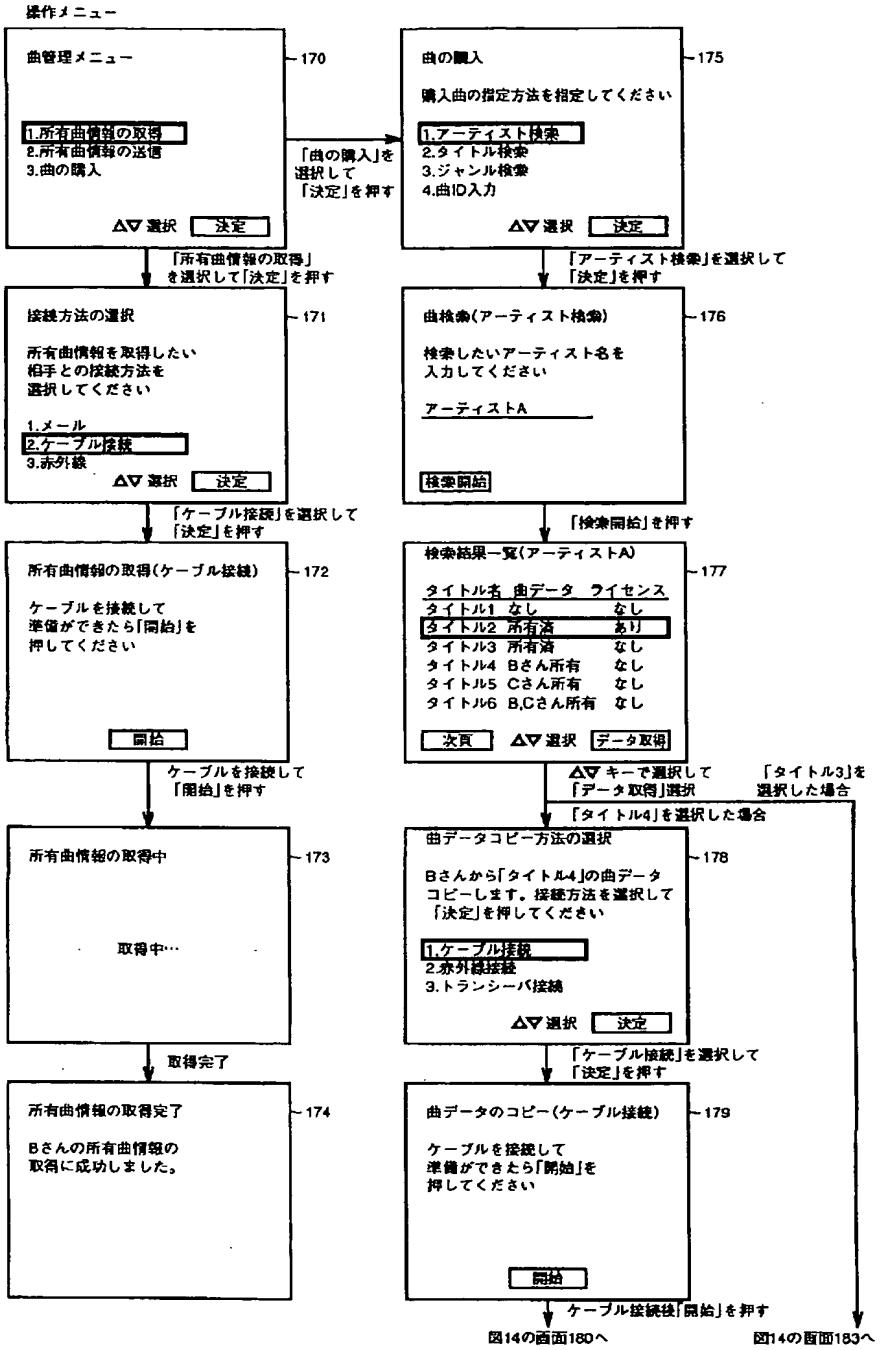
【図１１】



【図１９】

検索番号	コンテンツID	タイトル名	所有端末数	所有端末ID1	所有端末ID2	.....	ライセンス有無
1	CONTID(1)	タイトル(1)	0	0	0		0
2	CONTID(2)	タイトル(2)	1	端末ID1(2)	0		1
3	CONTID(3)	タイトル(3)	1	端末ID1(3)	0		0
4	CONTID(4)	タイトル(4)	1	端末ID1(4)	0		0
5	CONTID(5)	タイトル(5)	1	端末ID1(5)	0		0
6	CONTID(6)	タイトル(6)	2	端末ID1(6)	端末ID2(6)		0
⋮	⋮	⋮	⋮	⋮	⋮		⋮
S	CONTID(S)	タイトル(S)	0	0	0		0

【図１３】


操作メニュー
曲管理メニュー
170
1.所有曲情報の取得
2.所有曲情報の送信
3.曲の購入
△▽選択
決定
「曲の購入」を選択して「決定」を押す
曲の購入
175
購入曲の指定方法を指定してください
1.アーティスト検索
2.タイトル検索
3.ジャンル検索
4.曲ID入力
△▽選択
決定
「所有曲情報の取得」を選択して「決定」を押す
「アーティスト検索」を選択して「決定」を押す
接続方法の選択
171
所有曲情報を取得したい相手との接続方法を選択してください
1.メール
2.ケーブル接続
3.赤外線
△▽選択
決定
曲検索(アーティスト検索)
176
検索したいアーティスト名を入力してください
アーティストA
検索開始
「ケーブル接続」を選択して「決定」を押す
「検索開始」を押す
所有曲情報の取得(ケーブル接続)
172
ケーブルを接続して準備ができたら「開始」を押してください
開始
検索結果一覧(アーティストA)
177
タイトル名 曲データ ライセンス
タイトル1 なし なし
タイトル2 所有済 あり
タイトル3 所有済 なし
タイトル4 Bさん所有 なし
タイトル5 Cさん所有 なし
タイトル6 B,Cさん所有 なし
次頁
△▽選択
データ取得
ケーブルを接続して「開始」を押す
△▽キーで選択して「データ取得」選択
「タイトル3」を選択した場合
「タイトル4」を選択した場合
所有曲情報の取得中
173
取得中…
曲データコピー方法の選択
178
Bさんから「タイトル4」の曲データコピーします。接続方法を選択して「決定」を押してください
1.ケーブル接続
2.赤外線接続
3.トランシーバ接続
△▽選択
決定
取得完了
「ケーブル接続」を選択して「決定」を押す
所有曲情報の取得完了
174
Bさんの所有曲情報の取得に成功しました。
曲データのコピー(ケーブル接続)
179
ケーブルを接続して準備ができたら「開始」を押してください
開始
ケーブル接続後「開始」を押す
図14の画面180へ
図14の画面183へ

【図１４】

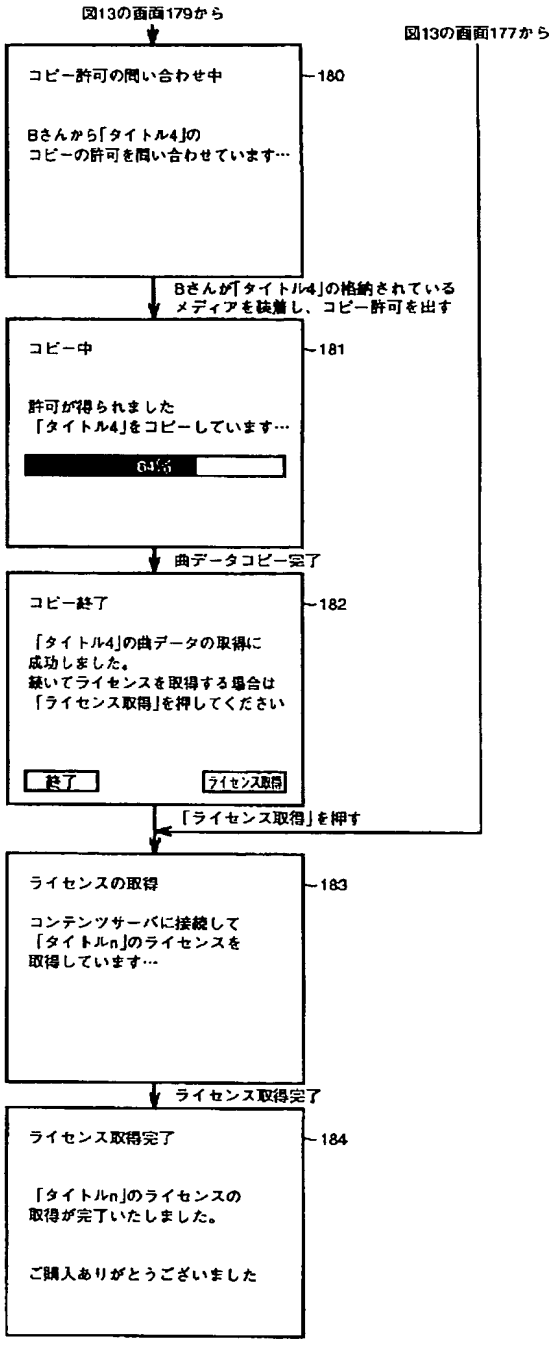
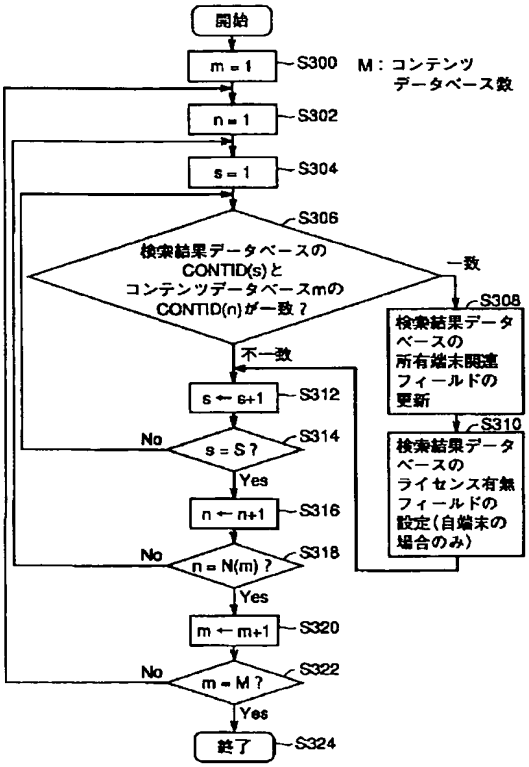
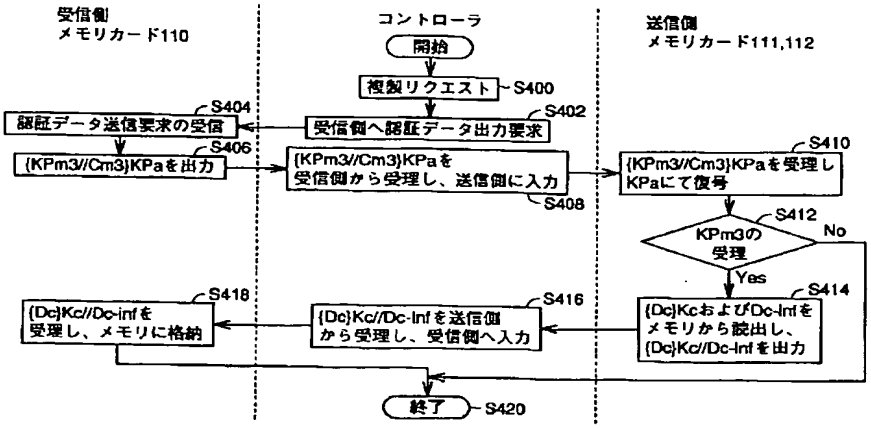


図13の画面179から
図13の画面177から
コピー許可の問い合わせ中
180
Bさんから「タイトル4」の
コピーの許可を問い合わせています…
Bさんが「タイトル4」の格納されている
メディアを装着し、コピー許可を出す
コピー中
181
許可が得られました
「タイトル4」をコピーしています…
曲データコピー完了
コピー終了
182
「タイトル4」の曲データの取得に
成功しました。
続いてライセンスを取得する場合は
「ライセンス取得」を押してください
終了
ライセンス取得
「ライセンス取得」を押す
ライセンスの取得
183
コンテンツサーバに接続して
「タイトルn」のライセンスを
取得しています…
ライセンス取得完了
ライセンス取得完了
184
「タイトルn」のライセンスの
取得が完了いたしました。
ご購入ありがとうございました

【図１７】


開始
m = 1
S300
M：コンテンツ
データベース数
n = 1
S302
s = 1
S304
S306
検索結果データベースの
CONTID(s)と
コンテンツデータベースmの
CONTID(n)が一致？
一致
不一致
S308
検索結果データ
ベースの
所有端末関連
フィールドの
更新
S310
検索結果データ
ベースの
ライセンス有無
フィールドの
設定(自端末の
場合のみ)
s ← s+1
S312
No
s = S？
S314
Yes
n ← n+1
S316
No
n = N(m)？
S318
Yes
m ← m+1
S320
No
m = M？
S322
Yes
終了
S324

【図２０】



フロントページの続き

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
Ｇ０６Ｆ	12/14	３２０	Ｇ０６Ｆ	12/14	３２０Ｅ
	17/30	１１０		17/30	１１０Ｆ
		１７０			１７０Ｚ
Ｈ０４Ｑ	7/38		Ｈ０４Ｂ	7/26	１０９Ｓ
Ｈ０４Ｌ	9/08		Ｈ０４Ｌ	9/00	６０１Ｂ

Ｆターム(参考)　5B017 AA06 BA09 CA16
5B075 ND16 PP23 PQ02
5B082 HA05
5J104 AA01 AA16 EA01 EA04 EA16
NA03 PA02 PA07
5K067 AA32 BB04 DD17 EE02 EE10
EE16 FF02 FF23 GG01 GG11
HH05 HH22 HH23 HH36

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.